



IntraCore[®] IC3624PWR

Layer 2+ Power over Ethernet (PoE) Switch
with Dual Gigabit

User's Manual



IntraCore® IC3624PWR

Layer 2+ Power over Ethernet (PoE) Switch
with Dual Gigabit

User's Manual

Asanté Technologies, Inc.
2223 Old Oakland Road
San Jose, CA 95131
USA

SALES

800-662-9686 Home/Office Solutions
800-303-9121 Enterprise Solutions
408-435-8388

TECHNICAL SUPPORT

801-566-8991: Worldwide
801-566-3787: Fax
www.asante.com/support
support@asante.com

[Default IP Address: 192.168.0.1]
[Default username: root]
[Default password: Asante]

Copyright © 2004 Asanté Technologies, Inc. All rights reserved. No part of this document, or any associated artwork, product design, or design concept may be copied or reproduced in whole or in part by any means without the express written consent of Asanté Technologies, Inc. Asanté and IntraCore are registered trademarks and the Asanté logo, AsantéCare, Auto-Uplink, and IntraCare are trademarks of Asanté Technologies, Inc. All other brand names or product names are trademarks or registered trademarks of their respective holders. All features and specifications are subject to change without prior notice.

Rev. A 10/22/04

Table of Contents

| | |
|--|----|
| Table of Contents..... | 3 |
| Chapter 1: Introduction..... | 7 |
| 1.1 Features | 7 |
| 1.1.1 Connectivity | 7 |
| 1.1.2 Performance | 8 |
| 1.1.3 Management..... | 8 |
| 1.2 Network Management Options | 8 |
| 1.3 Ports..... | 8 |
| Chapter 2: Network Planning | 9 |
| 2.1 Management Access Overview | 9 |
| 2.2 SNMP Access | 10 |
| 2.2.1 Protocols | 11 |
| Chapter 3: Hardware Installation and Setup | 12 |
| 3.1 Installation Overview | 12 |
| 3.2 Safety Recommendations | 12 |
| 3.3 Site Requirements..... | 13 |
| 3.3.1 Environmental Requirements..... | 13 |
| 3.3.2 Power..... | 13 |
| 3.3.3 Cooling and Airflow | 13 |
| 3.3.4 Rack Mounting | 13 |
| 3.4 Preparing for Installation..... | 14 |
| 3.5 Unpacking and Inspecting | 14 |
| 3.5.1 Recommended Tools..... | 15 |
| 3.6 Installing the Switch..... | 15 |
| 3.6.1 Mounting the Switch in a Rack..... | 15 |
| 3.6.2 Desktop or Shelf Mounting..... | 16 |

| | |
|---|----|
| 3.7 Applying Power | 16 |
| 3.8 Ethernet Cabling..... | 17 |
| 3.9 Connecting to the Console Port..... | 17 |
| 3.9.1 Wiring Map for Serial Cable | 18 |
| Chapter 4: Connecting Network Devices | 19 |
| 4.1 Twisted-Pair Devices..... | 19 |
| 4.1.1 Cable Guidelines..... | 19 |
| 4.1.2 Connecting to PCs, Servers, Hubs and Switches | 19 |
| 4.1.3 Network Wiring Connections..... | 20 |
| 4.2 Interpreting LEDs | 20 |
| 4.3 Connectivity Guidelines | 21 |
| 4.3.1 Fast Ethernet Ports | 21 |
| 4.3.2 Combo Ports | 21 |
| 4.4 Cable Labeling and Connection Records | 22 |
| Chapter 5: Configuring the Switch | 23 |
| 5.1 Connecting to the Switch..... | 23 |
| 5.2 Direct Access | 24 |
| 5.3 Initial Logon | 26 |
| Chapter 6: Using the Interface | 28 |
| 6.1 General Information Menu..... | 28 |
| 6.2 Basic Configuration Menu | 30 |
| 6.2.1 Administration Configuration..... | 31 |
| 6.2.2 IP Configuration | 32 |
| 6.2.3 SNMP Configuration | 32 |
| 6.2.4 Port Configuration | 37 |
| 6.2.6 Forwarding DB | 38 |
| 6.2.7 Sntp Configuration | 39 |
| 6.2.8 ARP Table..... | 40 |

| | |
|--|----|
| 6.3 Advanced Switch Configuration..... | 41 |
| 6.3.1 VLAN Management..... | 42 |
| 6.3.2 Link Aggregation | 45 |
| 6.3.3 Port Monitoring..... | 47 |
| 6.3.4 MSTP Configuration..... | 47 |
| 6.3.5 Access List Configuration..... | 56 |
| 6.3.6 Quality of Service Configuration..... | 63 |
| 6.3.7 Storm Control..... | 64 |
| 6.3.8 802.1 Port Based Access Control | 65 |
| 6.3.9 IGMP Snooping..... | 66 |
| 6.3.10 Power over Ethernet | 68 |
| Map: Main Menu->Advanced Switch Configuration->Power over Ethernet | 68 |
| 6.4 Statistics | 71 |
| 6.5 Tools | 72 |
| 6.5.1 TFTP Software Upgrade | 72 |
| 6.5.2 Configuration File Upload/Download..... | 73 |
| 6.5.3 System Reboot | 74 |
| 6.5.4 Ping Execution | 74 |
| 6.5.5 System Log | 75 |
| 6.6 Save Configuration | 76 |
| 6.7 Run CLI | 76 |
| Appendix A: Basic Troubleshooting | 77 |
| A.1 Diagnosing Switch Indicators | 77 |
| A.2 Power and Cooling Problems..... | 77 |
| A.3 Installation..... | 77 |
| A.4 In-Band Access..... | 77 |
| Appendix B: Specifications..... | 79 |
| Appendix C: Cables and Pin Assignments..... | 81 |
| C.1 Twisted-Pair Cable and Pin Assignments..... | 81 |
| C.1.1 Pin Assignments for 10BaseT/100BaseTX..... | 81 |
| C.1.2 Straight-Through Wiring | 82 |
| C.1.3 Crossover Wiring..... | 82 |

C.2 Pin Assignments for 1000BaseT Pin 82

C.3 Cable Testing for Existing Category 5 Cable 83

 C.3.1 Adjusting Existing Category 5 Cabling to Run 1000BaseT..... 83

C.4 Fiber Standards 83

Appendix D: FCC Compliance and Warranty Statements..... 85

 D.1 FCC Compliance Statement 85

 D.2 Important Safety Instructions 85

 D.3 IntraCore Warranty Statement 86

Appendix E. Online Warranty Registration..... 87

Chapter 1: Introduction

The IntraCore IC3624PWR Layer 2+ Power over Ethernet (PoE) with Dual Gigabit (IC3624PWR) is a product you can use to build your next generation network.

The IC3624PWR device uses Layer 2+ technology and has 24 ports for 10/100/1000BaseTX Fast Ethernet with 2 combination ports for added 10/100BaseT Gigabit Ethernet.

Use the advanced features on the IC3624PWR switch to deploy Voice over IP (VoIP) telephones, cameras and wireless access points.

The following figure shows the front of the IC3624PWR PoE switch.



1.1 Features

The IntraCore IC3624PWR supports the following features:

1.1.1 Connectivity

Compared with conventional 24-port 10/100 Fast Ethernet Layer 2+ switches, the IC3624PWR delivers power for all compatible devices.

- Meets IEEE 802.3af PoE standards
- 180 watts of total power (up to 15.4 watts per 10/100 port)
- IEEE 802.1p prioritization, DiffServ and IP ToS supports VoIP.

The switch supports all the services needed for your advanced network.

- Supports 802.1x authentication per port
- Up to 256 VLANs with GVRP and GARP
- 4 class of service queues per port
- IGMP v1 and v2 snooping support
- 6 groups of trunking for link aggregation and redundancy
- IEEE 802.1d and 802.1s spanning tree support with rapid reconfiguration and fast link option

1.1.2 Performance

The IC3624PWR switch uses a wire-speed, non-blocking switching fabric.

- Wire-speed Gigabit switching (1,488,000 pps) and Fast Ethernet switching (148,800 pps)
- Non-blocking 8.8 Gbps switch fabric

1.1.3 Management

- Web browser
- Telnet (multiple sessions)
- Console
- SNMP v1 and v2c
- RMON Groups 1, 2, 3 and 9

1.2 Network Management Options

The IntraCore IC3624PWR provides both local and remote management. You can configure or monitor the switch using the embedded management software or by using SNMP applications. You can manage the switch by a direct connection to the RS-232 console port (out-of-band), or a network connection (in-band) using Telnet, or the on-board Web agent.

1.3 Ports

Each port has auto-negotiation, so the optimum transmission mode (half or full duplex), and data rate (10, 100, or 1000 Mbps) is always available. If a device connected to one of these ports does not support auto-negotiation, the communication mode of that port can be manually configured.

Each port also supports auto-negotiation of flow control, so the switches can automatically prevent port buffers from becoming saturated.

Chapter 2: Network Planning

This chapter gives an overview of switch management, including the methods you can use to manage your IntraCore IC3624PWR Managed Switch. Topics include:

- Management Access Overview
- SNMP Access
- Protocols

2.1 Management Access Overview

You can access and manage the IC3624PWR Managed Switch using the following methods:

- Administration console
- Web browser interface
- External SNMP-based network-management application

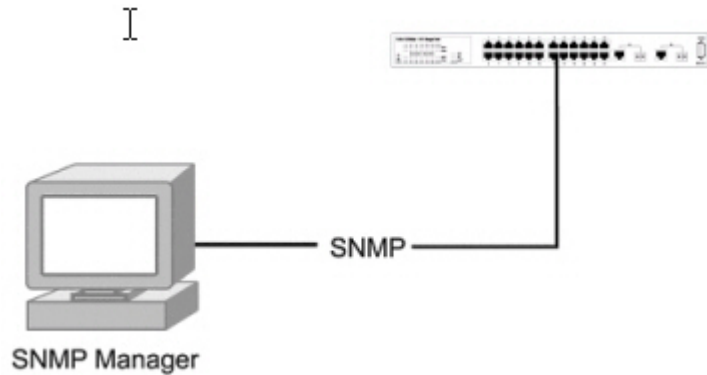
The administration console and Web browser interface support are embedded in the switch's firmware and available for immediate use. Use the following table to determine which method is best suited for your network environment.

| Management Method | Advantages | Disadvantages |
|------------------------|--|---|
| Administration Console | <p>Out-of-band access through direct cable connection eliminates network bottlenecks, crashes, and downtime</p> <p>No IP address or subnet is needed</p> <p>Menu or CLI based</p> <p>HyperTerminal access to full functionality (standard Microsoft Windows 95/98/NT/2000 operating systems)</p> | <p>Must be near switch or use dial-up connection</p> <p>Not convenient for remote users</p> <p>Not available using a GUI</p> |
| Web Browser or Telnet | <p>Access from any location through the switch's IP address</p> <p>Configure the switch remotely</p> <p>Compatible with Internet Explorer and Netscape Navigator Web browsers</p> <p>GUI data available</p> <p>Menu or CLI interfaces available</p> | <p>Security can be compromised</p> <p>Lag times on poor connections are possible</p> <p>GUI display may slow navigation</p> |
| SNMP Agent | <p>Communicate at the Management Information Base (MIB) level</p> <p>Based on open standards</p> | <p>Requires SNMP manager software</p> <p>Limited amount of information available</p> <p>Some settings require calculations</p> <p>Security can be compromised (hackers need only know the community name)</p> |

2.2 SNMP Access

You can use an external Simple Network Management Protocol (SNMP) based application to manage your IC3624PWR switch.

This management method requires the SNMP agent on the switch and the SNMP Manager station to use the same community string. Before using this method, enter the SNMP Manager station in the SNMP Host table on the switch. This management method uses two community strings: the GET community string and the SET community string. If the SNMP Manager only knows the SET community string, it can both read and write to the MIBs. If the SNMP Manager only knows the GET community string, it only reads the MIB. The default GET community string for the switch is **public**, and the host table is empty. The following figure is an example of this management method.



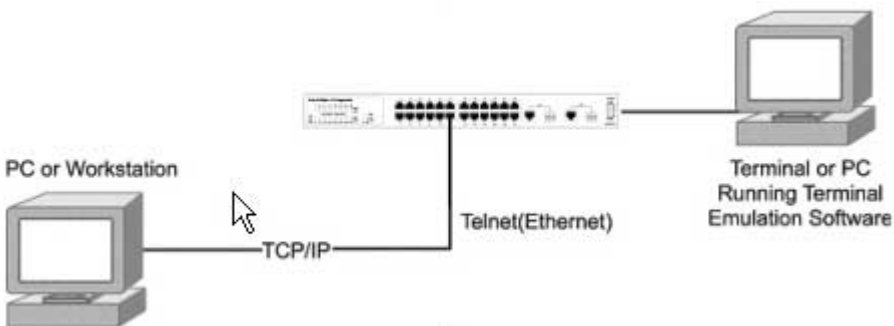
2.2.1 Protocols

The IC3624PWR switch supports the following protocols:

- Virtual terminal protocols, such as Telnet
- SNMP
- Virtual Terminal Protocols

A virtual terminal protocol is a software program, such as Telnet, that allows you to establish a management session from a Macintosh, a PC, or a UNIX workstation. Because Telnet runs over TCP/IP, you must have at least one IP address configured on the IC3624 switch before you can establish a connection.

When using the terminal emulation method you must connect a terminal or PC directly to the console port. The following figure shows a UNIX workstation connected to the system through a virtual terminal protocol (Telnet), and a terminal connecting directly to the console port through a null-modem cable.



SNMP Protocol

SNMP is the standard management protocol for multi-vendor IP networks. SNMP supports transaction-based queries that allow the protocol to format messages and to transmit information between reporting devices and data-collection programs. SNMP runs on top of the User Datagram Protocol (UDP), offering a connectionless-mode service.

Chapter 3: Hardware Installation and Setup

This chapter describes the procedures for rack-mounting, connecting the cables, and powering up the IntraCore IC3624PWR PoE switch at your site.

3.1 Installation Overview

1. Follow these steps to install the IntraCore IC3624PWR PoE switch:
2. Open the box and check the contents. For a complete list of the items included with the switch see “Equipment Checklist” section later in this chapter.
3. Install the switch in an equipment or wall rack, or prepare for desktop placement.
4. Connect the power cord to the switch and to an appropriate power source.
5. Connect network devices to the switch.

See the sections below for more detailed installation instructions.

3.2 Safety Recommendations

The following information provides safety guidelines to ensure general safety and to protect the switch from damage.

Note: The following guidelines may not include every possible hazard to which you may be exposed. Use caution when installing this switch. Only trained and qualified personnel install or replace this equipment.

- Keep the switch clean
- Keep tools and components off the floor and away from foot traffic
- Do not wear rings or chains (or other jewelry). Metal objects can heat up and cause serious injury to persons and damage to the equipment.
- Do not wear loose clothing. Fasten your tie or scarf and roll up your sleeves.
- When working with electricity, follow these guidelines:
- Disconnect all external cables before installing or removing the cover
- Do not work alone when working with electricity
- Always check that the cord has been disconnected from the outlet before performing hardware configuration
- Do not tamper with the equipment. Doing so could void the warranty
- Examine the work area for potential hazards (such as wet floors or ungrounded cables)

3.3 Site Requirements

Consider the following site requirements for proper installation.

3.3.1 Environmental Requirements

Choose a clean, dry, dust-free area location. Avoid direct sunlight, heat sources, or areas with high levels of electromagnetic interference. Failure to observe these limits may cause damage to the switch and may void the warranty.

3.3.2 Power

Make sure the power source adheres to the following guidelines:

Outlet: Properly grounded, located near the switch, and easily accessible

Power: Auto Switching 100-240 VAC, 50/60 Hz, maximum 225 watts

Frequency range: 50/60 Hz

3.3.3 Cooling and Airflow

The IC3624PWR PoE switch use internal fans for air-cooling. Do not restrict airflow by covering or obstructing air vents on the sides of the switch.

Operating Temperature: 32° to 104°F (0° to 40°C)

Relative Humidity: 10% to 90% non-condensing

3.3.4 Rack Mounting

Before mounting the switch in a rack follow these general precautions:

Size: 17.3 x 9.9 x 1.7 in (440 x 253 x 43 mm)

Weight: 9.5 lb (4.3 kg)

Temperature: The temperature within a rack assembly may be higher than the ambient room temperature check that the rack-environment temperature is within the specified operating temperature range remains below 104°F (40°C).

Clearance: Clear all obstructions, such as other equipment or cables, block airflow to or from the vents of the switch. Be sure there is adequate clearance for servicing the switch.

Mechanical Loading: Do not place any equipment on top of a rack-mounted unit.

Circuit Overloading: Be sure that the supply circuit to the rack assembly is not overloaded.

Grounding: Rack-mounted equipment should be properly grounded. Particular attention should be given to supply connections other than direct connections to the mains.

3.4 Preparing for Installation

Switches can be mounted in a standard 19-inch equipment rack or on a flat surface. Follow these general precautions when planning your equipment locations and connections.

The site needs the following:

- Centrally located to the devices you want to link
- Near a power outlet.
- Constant temperature within 32° to 104°F (0° to 40°C) and its humidity within 10% to 90%, non-condensing
- Adequate space (approximately 2 in or 5 cm) on all sides for proper air flow
- Accessible for installing, cabling and maintaining the devices
- Clearly visible status LEDs

Additional precautions:

- Keep the front of the chassis free from obstruction and away from the exhaust air of other equipment. Electrical equipment generates heat and the ambient room temperature be enough to cool the equipment to required operating temperatures.
- Make sure twisted-pair cable is always routed away from power lines, fluorescent lighting fixtures and other sources of electrical interference, for example radios and transmitters.
- Make sure that the unit is connected to a separate grounded power outlet that provides 100 to 240 VAC, 50 to 60 Hz, is within 8 ft (2.44 m) of each device and is powered from an independent circuit breaker. As with any equipment, using a filter or surge suppressor is recommended.

3.5 Unpacking and Inspecting

Before you unpack your equipment examine all shipping containers for damage. If any damage has occurred, notify the shipping carrier immediately. Unpack the unit by removing the packing material and lifting it from the protective enclosures. Visually examine the equipment and check the container for parts and accessories. You should have the following items:

- An IntraCore IC3624PWR PoE switch
- Four adhesive foot pads
- A Rack Mounting Kit
 - Two brackets
 - Four screws for attaching the brackets
- An AC Power Cord
- An RS-232 console cable

Contact your dealer immediately if any item is missing.

3.5.1 Recommended Tools

You need the following tools and equipment (not included) to install the switch into an equipment rack:

- Flat head screwdriver
- Phillips head screwdriver
- Four mounting screws for each device you plan to install in a rack (not included with the switch)
- Antistatic mat or foam

3.6 Installing the Switch

The switch can be mounted in a standard 19-inch equipment rack or place on a desktop or shelf. Mounting instructions for each type of site follow.

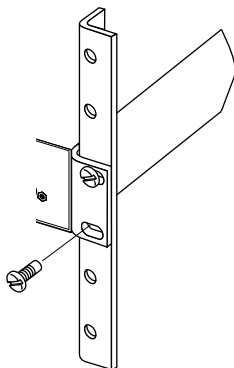
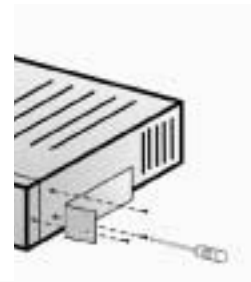
3.6.1 Mounting the Switch in a Rack

When installing this unit in an empty rack, mount it at the bottom. When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom. Follow these steps to properly install the switch into an equipment rack.

Caution: Before continuing, disconnect all cables from the switch.

To mount the switch onto an equipment rack:

- Place the switch on a flat, stable surface.
- Locate a rack-mounting bracket (supplied) and place it over the mounting holes on one side of the switch.
- Use the screws (supplied) to secure the bracket (with a Phillips screwdriver).
- Repeat the two previous steps on the other side of the switch.
- Place the switch in the equipment rack.
- Secure the switch attaching the mounting brackets onto the equipment rack with the screw supplied with the unit.



Warning: Make sure you support the switch until all the mounting screws for each bracket is secured to the equipment rack. Failure to do so could cause the switch to fall, which may result in personal injury or damage to the switch.

When installing multiple switches, mount them in the rack, one below the other, in any order.

When installation is complete turn to the “Applying Power” section.

3.6.2 Desktop or Shelf Mounting

Follow these steps when planning to use the switch on either a desktop or a shelf:

1. Attach the four adhesive feet to the bottom of the switch.
2. Set the device on a flat surface near an AC power source, making sure there are at least two inches of space on all sides for proper airflow.
3. Place each device squarely on top of the one below, in any order.

When installation is complete refer to the “Applying Power” section.

3.7 Applying Power

The system’s front panel LED display allows you to monitor the status of the switch. Follow these steps to connect the switch.

1. Use the supplied power cord and plug the female end directly into the receptacle located at the back of the device.
2. Plug the other end of the cord into a properly grounded electrical outlet.
3. Check the front-panel LEDs as the device is powered on to be sure the Power LED is lit. If not lit, check that the power cable is correctly plugged in.
4. Connect the optional redundant power supply to the switch and to an AC power source by following the instructions for the unit.

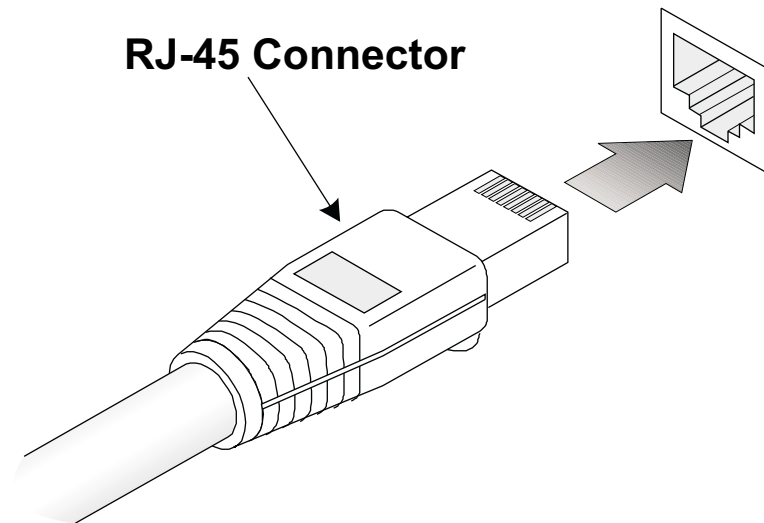
Warning: For International use: if you use power other than AC, you must use power cords that meet the appropriate standards for the power you are using.

3.8 Ethernet Cabling

The cables you need are determined by the existing equipment.

To ensure proper operation when installing the switch into a network, make sure that the current cables are suitable with either 10/100BaseTX, 10/100/1000BaseT or 1000BaseT operation. Check the following criteria against the current installation of your network:

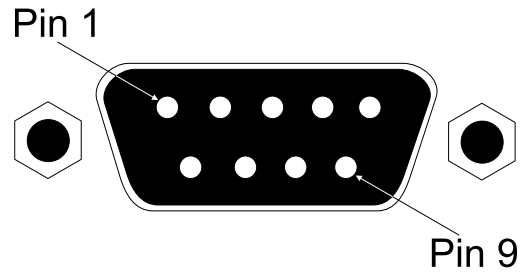
- **Cable type:** Unshielded twisted pair (UTP) or shielded twisted pair (STP) cables with RJ-45 connectors; Category 3 or better for 10BaseT and Category 5 or better for 100BaseTX.
- Protection from radio frequency interference emissions
- Electrical surge suppression
- Separation of electrical wires (switch related or other) and electromagnetic fields from data based network wiring
- Safe connections with no damaged cables, connectors, or shields



When attaching a workstation to the switch, a standard straight-through CAT5 cable may be used.

3.9 Connecting to the Console Port

The DB-9 serial port located on the front panel is used to connect to the switch for out-of-band console configuration. The on-board configuration program can be accessed from a terminal or a PC running a terminal emulation program. The pin assignments used to connect to the serial port are provided in the following tables.



3.9.1 Wiring Map for Serial Cable

The following table describes the serial cable wiring information.

| Switch's 9-Pin Serial Port | Null Modem | PC's 9-Pin DTE Port |
|----------------------------|------------|------------------------|
| 2 RXD (receive data) | ← | 3 TXD (transmit data) |
| 3 TXD | → | 2 RXD (receive data) |
| 5 SGND (signal ground) | --- | 5 SGND (signal ground) |

The serial port configuration requirements are as follows:

- Default Baud rate—9,600 bps
- Character Size—8 Characters
- Parity—None
- Stop bit—One
- Data bits—8

Chapter 4: Connecting Network Devices

The switch is designed to interconnect multiple segments (or collision domains). It can be connected to network cards in PCs and servers, and to hubs, routers, or other switches.

4.1 Twisted-Pair Devices

Each device requires an unshielded twisted-pair (UTP) cable with RJ-45 connectors at both ends. Use Category 5 for 100BaseTX connections, and Category 3, 4 or 5 for 10BaseT connections.

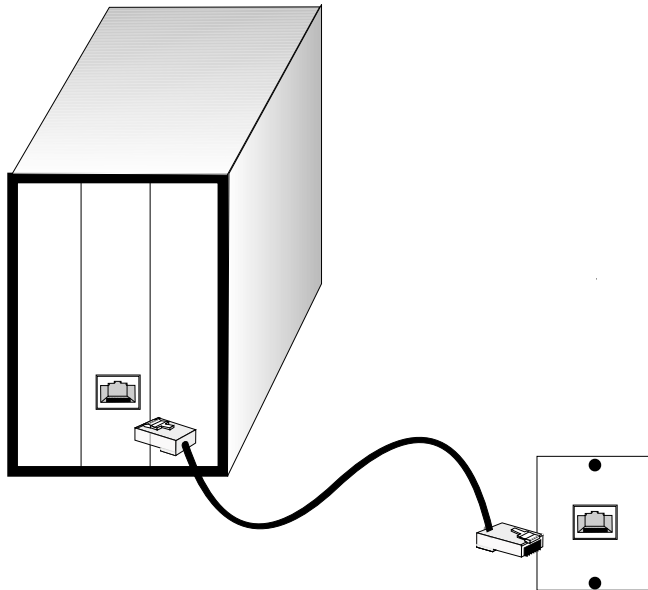
4.1.1 Cable Guidelines

The RJ-45 ports on these switches support automatic MDI/MDI-X pinout configuration, so you can use standard straight-through twisted-pair cables to connect to any other network device (PCs, servers, switches, routers, or hubs).

Caution: Do not plug a phone jack connector into an RJ-45 port. Doing this will damage the switch. Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

4.1.2 Connecting to PCs, Servers, Hubs and Switches

Attach one end of a twisted-pair cable segment to the device's RJ-45 connector.



If the device is a PC card and the switch is in the wiring closet, attach the other end of the cable segment to a modular wall outlet that is connected to the wiring closet. (See “Network Wiring Connections” later in this chapter.) Otherwise, attach the other end to an available port on the switch.

Make sure each twisted pair cable does not exceed 100 meters (328 ft) in length.

As each connection is made, the Link LED (on the switch) corresponding to each port lights up to indicate that the connection is complete. (For more LED information see, “Interpreting LEDs” later in this chapter.)

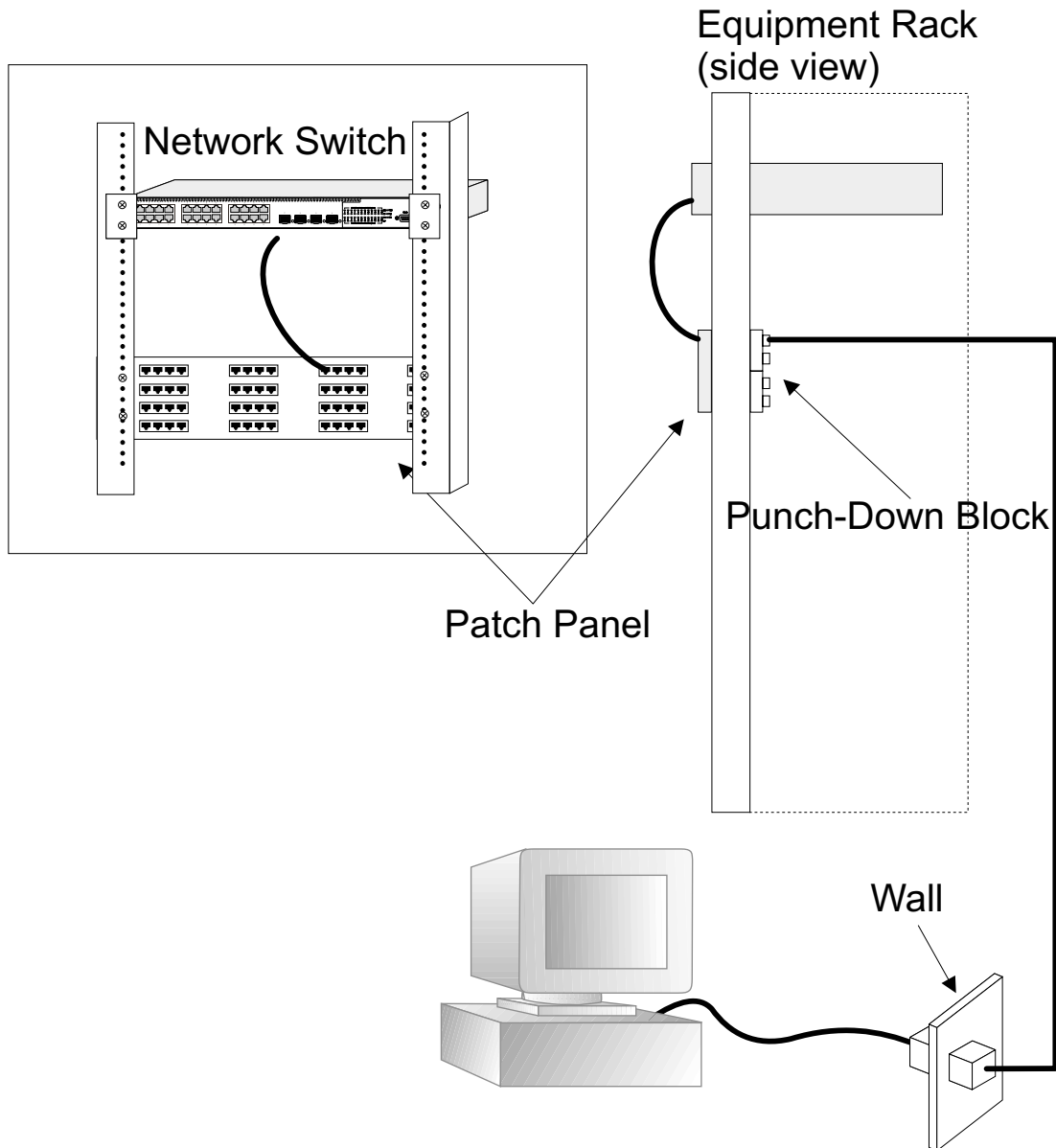
4.1.3 Network Wiring Connections

The punch-down block is an integral part of many of the newer equipment racks. It is actually part of the patch panel. Instructions for making connections in the wiring closet with this type of equipment follows.

Attach one end of a patch cable to an available port on the switch, and the other end to the patch panel.

Attach one end of a cable segment to the back of the patch panel where the punch-down block is located, and the other end to a modular wall outlet.

Label the cables to simplify future troubleshooting.



4.2 Interpreting LEDs

The LEDs are located on the front panel.

The following table lists the LEDs and describes the status lights.

| LED | Condition | Status |
|-------------------------|-----------|---|
| Fast Ethernet | On/Green | The port has a valid 100 Mbps link. Flashing indicates activity. |
| | On/Amber | The port has a valid 10 Mbps link. Flashing indicates activity. |
| Gigabit Ethernet | On/Green | The port has a valid 100 Mbps or 1000 Mbps link. Flashing indicates activity. |

4.3 Connectivity Guidelines

When adding to your network, follow the connectivity rules listed in the manuals for these products. Since the switch breaks the path for connected devices into separate collision domains, you should not include the switch or connected cabling in your calculations for cascade length involving other devices.

4.3.1 Fast Ethernet Ports

There are 24 10/100BaseTX ports. The following table shows the connection types, cables, maximum lengths, and required connectors.

| Connection Type | Cable | Length | Connector |
|-----------------|---|----------------|-----------|
| 100 BaseTX | Category 5 or better 100-ohm UTP or STP | 100 m (328 ft) | RJ-45 |

4.3.2 Combo Ports

There are two combo ports for use with 10/100/100 BaseT or Gigabit Ethernet ports. The following table shows the cable, maximum length, and required connectors.

| Cable | Length | Connector |
|--|----------------|-----------|
| Twisted Pair, Categories 3, 4, 5 or better 100-ohm UTP | 100 m (328 ft) | RJ-45 |

4.4 Cable Labeling and Connection Records

When planning a network installation, it is essential to label and record where each cable is connected. This helps you locate inter-connected devices, isolate faults, and change your topology.

To manage the physical implementations of your network, follow these guidelines:

- Label the opposing ends of each cable.
- Draw a map of the location of all network-connected equipment using your building's floor plans. For each piece of equipment, identify devices on the connection.
- Note the length of each cable and the maximum cable length supported by the switch ports.
- Use a location-based key when assigning prefixes to your cable labeling.
- Use sequential numbers for cables that originate from the same equipment.
- Name racks to help differentiate between them.
- Label each piece of equipment.
- Display a copy of your equipment map, including keys to all abbreviations, at each equipment rack.

Chapter 5: Configuring the Switch

This chapter takes you through the steps required to initially connect the switch to a console, set up initial passwords, configure an IP address, and restore factory defaults. For complete information about configuring, monitoring, and maintaining your switch, refer to the System Management Guide.

5.1 Connecting to the Switch

The switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON and a Web-based interface. You can connect PC directly to the switch for configuration and monitoring via a command line interface (CLI).

Note: The IP address for this switch is unassigned by default. To change this address, see the “Setting an IP Address” section.

The switch’s HTTP Web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard Web browser such as Netscape Navigator version 6.2 and higher or Microsoft IE version 5.0 and higher. You can access the switch’s Web management interface from any computer attached to the network.

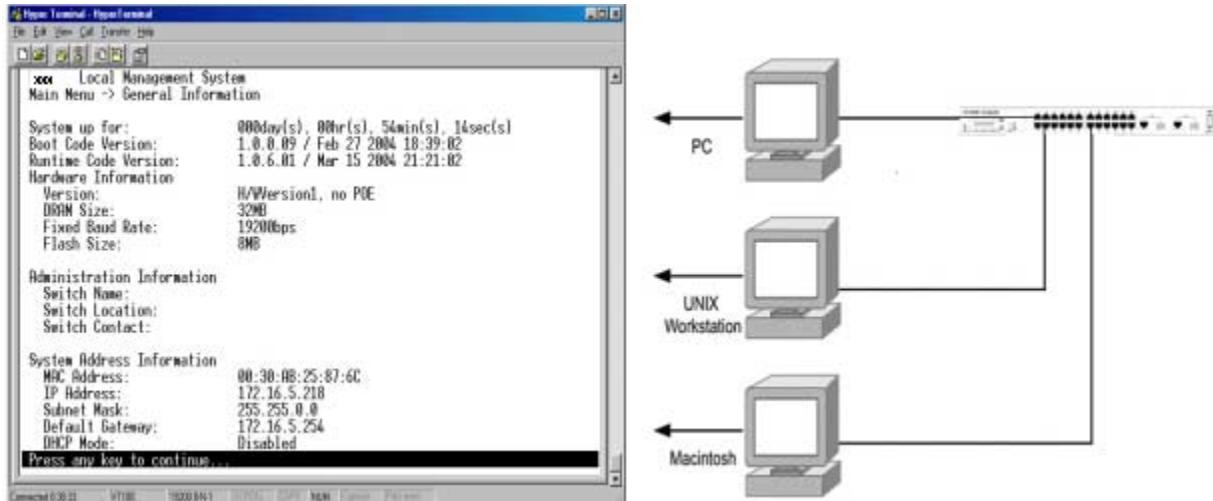
Access the CLI program by using a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet connection over the network.

The switch’s management agent also supports SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using network management software such as HP OpenView.

The switch’s Web interface, CLI configuration program, and SNMP agent allow you to perform different management functions including:

- Set user names and passwords
- Set an IP interface for a management VLAN
- Configure SNMP parameters
- Enable/disable any port
- Set the speed/duplex mode for any port

The administration console is an internal, character-oriented, VT-100/ANSI menu-driven user interface for performing management activities. Using this method, you can view the administration console from a terminal, PC, Apple Macintosh, or UNIX workstation connected to the switch’s console port. The following figure shows an example of this management method.



5.2 Direct Access

Direct access to the switch console is achieved by connecting the switch's console port to a VT-100 or compatible terminal or to a PC, Apple Macintosh, or UNIX workstation equipped with a terminal-emulation program. This connection is made using the null-modem cable supplied with the switch.

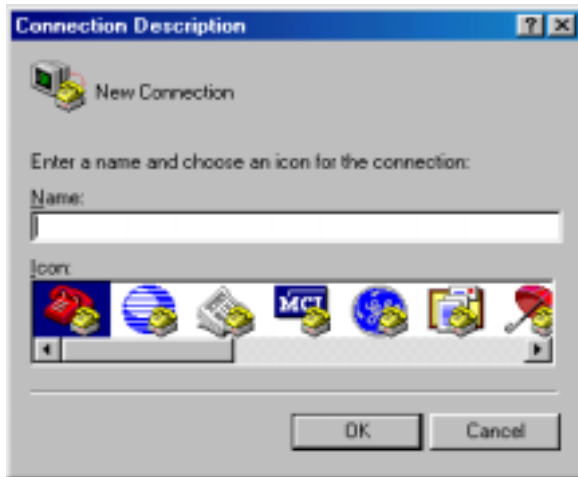
The following list provides examples of terminal-emulation programs:

- HyperTerminal (which is built into the Microsoft Windows operating systems)
- ZTerm (Apple Macintosh)
- TIP (UNIX workstation)

Follow these steps to set up the connection. Note; the graphics in this example show the HyperTerminal on a PC.

1. Click the Start button.
2. Select Accessories and then Communications.
3. Select HyperTerminal

The following screen appears.



1. Enter a name for this connection.

2. Click OK

The following screen appears.



1. In the drop down box labeled Connect Using:, click the arrow and choose the desired COM port. (In the example below, COM1 is the port selected.)

2. Click OK.

Connection Settings

The port settings are as follows:

| | |
|---------------|------|
| Baud Rate: | 9600 |
| Data Bits: | 8 |
| Parity: | None |
| Stop Bits: | 1 |
| Flow Control: | None |



1. Enter the settings.
2. Click OK.

5.3 Initial Logon

The switch offers a Command Menu Interface (CMI), which is a menu-driven method for managing the switch, as well as a Command Line Interface (CLI), which uses text input to manage the switch. Unless otherwise noted, the screen examples in this chapter are from the CLI.

When the HyperTerminal window opens and you are connected to the switch the following screen appears. If you do not get a login screen or main menu, press the return key.



To use the arrow keys when attached to the User Interface using a Telnet Session, under the terminal pull down menu choose Properties and activate the VT100 Arrows option.

Chapter 6: Using the Interface

The main menu displays available sub-menus. The letter within square bracket of each menu option can be typed to directly choose that option. From the main menu there are seven menu items to choose from:

- General Information
- Basic Configuration
- Advanced Switch Configuration
- Statistics
- Switch Tools Configuration
- Save Configuration
- Run CLI

To logout of the user interface, press the Ctrl and D keys at anytime during your telnet session. You return to the login screen (password enabled) or Main Menu (password disabled).

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System

Main Menu

[G]eneral Information
[B]asic Switch Configuration...
[A]dvanced Switch Configuration...
[S]tatistics
Switch [T]ools Configuration...
Save Configuration to [F]lash
Run [C]LI
[Q]uit

Command> 
Enter the character in square brackets to select option

```

6.1 General Information Menu

The General Information Menu allows you to review information about the switch. Following are two examples of this screen. The first example shows the screen using the GUI interface the second example shows using the interface from a telnet session.

The image displays the ASANTE IC3624PWR Remote Management System interface. The top header features the ASANTE logo and a navigation bar with icons for various system functions. Below the header, a sidebar on the left lists menu options: General Info., Basic Config., Advanced Config., and Tools. The main content area is titled "General Information" and displays the following data:

| General Information | |
|----------------------------|---------------------------------|
| System Up Time: | 0 day 5 hr 47 min 28 sec |
| Boot Code Version/Date: | 1.0.0.13 / Mar 26 2004 11:07:20 |
| Runtime Code Version/Date: | 1.0.0.02 / Oct 14 2004 10:42:43 |
| Hardware Information | |
| Revision: | Version1 |
| DRAM Size: | 32 MB |
| Flash Size: | 8 MB |
| Console Baud Rate: | 9600 bps |
| Administration Information | |
| System Name: | |
| System Location: | |
| System Contact: | |
| System Address Information | |
| MAC Address: | 00:30:AB:25:8C:31 |
| IP Address: | 69.226.6.75 |
| Subnet Mask: | 255.255.255.0 |
| Default Gateway: | 69.226.6.78 |
| DHCP Mode: | Disabled |

Below the main interface is a terminal window titled "Terminal — telnet — 80x24". The terminal output shows the system's main menu and the selected "General Information" screen, mirroring the data shown in the main interface. A black bar with the text "Press any key to continue..." is visible over the terminal output.

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Main Menu -> General Information

System up for:          000day(s), 00hr(s), 06min(s), 27sec(s)
Boot Code Version:     1.0.0.13 / Mar 26 2004 11:07:20
Runtime Code Version:  1.0.0.00 / Sep 21 2004 13:53:25
Hardware Information
  Version:              Version1
  DRAM Size:            32MB
  Fixed Baud Rate:     9600bps
  Flash Size:          8MB
Administration Information
  Switch Name:
  Switch Location:
  Switch Contact:

System Address Information
  MAC Address:         00:30:AB:25:8C:31
  IP Address:          192.108.250.81
  Subnet Mask:         255.255.255.0
  Default Gateway:    192.108.250.5
  DHCP Mode:          Disabled
  
```

The following table describes the areas you see from the General Information screen.

| Heading | Description |
|---|--|
| System up Time | System run time after boot up |
| Boot Code Version Date | The version and timestamp of boot code |
| Runtime Code Version Date | The version and timestamp of runtime code |
| Hardware Information Version DRAM Size Fixed Baud Rate Flash Size | Hardware associated information Hardware revision version Size of DRAM on system Data rate on console port, set to 19200 Size of Flash memory |
| Administration Information System Name System Location System Contact | Name of system (user defined) Location of system (user defined) Contact information (user defined) |
| System Address Information MAC Address IP Address Subnet Mask Default Gateway DHCP Mode | MAC Address of system Default IP address (user defined) Default Subnet mask (user defined) Default gateway (user defined) Enabled/Disabled DHCP function |

6.2 Basic Configuration Menu

The Basic Configuration screen allows you to configure several basic system-related settings for future use. You reach this screen from the Main Menu.

There are eight submenus at Basic Configuration Menu.

- Administration Configuration
- IP Configuration
- SNMP Configuration
- Port Configuration
- System Security
- Forwarding DB
- SNTP Configuration
- ARP Table
- Quit to previous menu

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Main Menu -> Basic Switch Configuration Menu

System [A]dministration Configuration
System [I]P Configuration
S[N]MP Configuration
[P]ort Configuration
[S]ystem Security Configuration
[F]orwarding Database
SN[T]P Configuration
A[R]P Table
[Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

6.2.1 Administration Configuration

From the Admin Configuration screen, you can enter system-related information for reference such as System Name, System Location, and System Contact Information.

Map: Main Menu->Basic Configuration Menu->Administration Configuration

Note: The system Description and Object ID are not configurable.

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Basic Switch Configuration -> System Admin. Configuration Menu

Description: IntraCore 3624PWR
Object ID: 1.3.6.1.4.1.298.2.2.35
Name:
Location:
Contact:

----- <COMMAND> -----

Set System [N]ame
Set System [L]ocation
Set System [C]ontact Information
[Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

6.2.2 IP Configuration

All hosts that run IP must have a unique IP address. An IP address is a logical address that is independent of a host's hardware. IP addresses are 32 bits long.

Map: Main Menu->Basic Configuration Menu->IP Configuration

From the IP Configuration screen you can manage the IP related information of the system.

The two IP assignment modes are:

Manual – You manually enter IP related information

DHCP – The switch accepts DHCP broadcast from a DHCP server and automatically configures IP related information

In manual mode, you need a site-specific IP address to configure the IP address, Gateway Address, and Network Mask (or subnet mask). Consult your network administrator.

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Basic Switch Configuration -> System IP Configuration Menu

MAC Address:      00:30:AB:25:8C:31
IP Address:       69.226.6.73
Subnet Mask:     255.255.255.0
Default Gateway: 69.226.6.78
DHCP Mode:       Disabled

----- <COMMAND> -----

Set [I]P Address
Set Subnet [M]ask
Set Default [G]ateway
Set [D]HCP Status
Set DHCP [R]enew
[Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

6.2.3 SNMP Configuration

The Simple Network Management Protocol (SNMP) is an application-layer protocol designed to facilitate the exchange of management information between network devices. By using SNMP-transported data (such as packets per second and network error rates), network administrators can manage network performance, find and solve network problems, and plan for network growth.

You can manage the switch using the SNMP from a network management station.

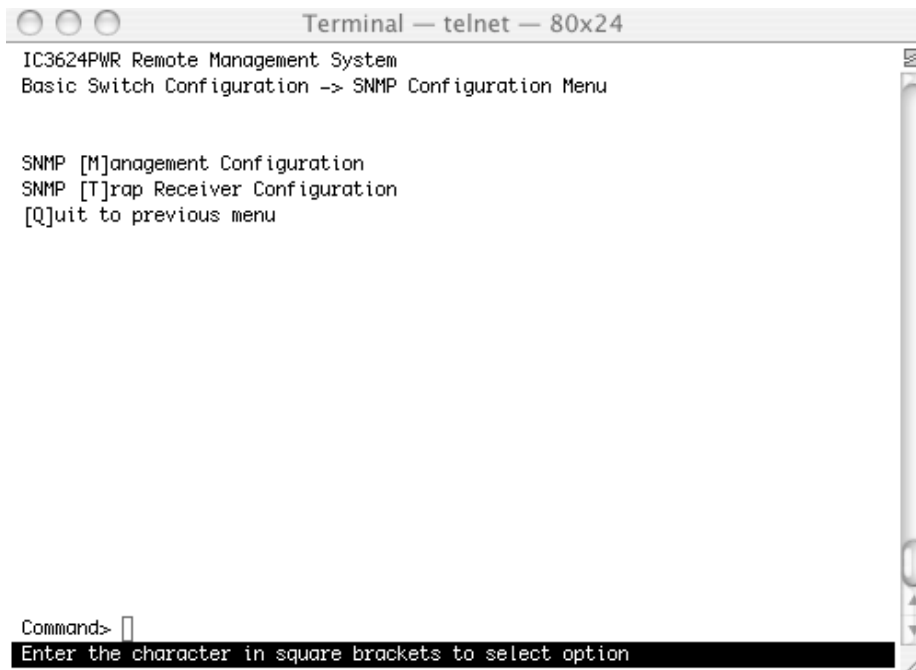
Map: Main Menu->Basic Configuration Menu->SNMP Configuration

Configure the switch by adding the SNMP host agent to the host table in order to participate in the SNMP community. SNMP management features on the switch include:

- Simple Network Management Protocol (SNMP)
- Support Standard MIBs:
 - MIB II (RFC1213)
 - Ethernet Interface MIB (RFC1643)
 - Bridge MIB (RFC1493)
 - Private Enterprise MIB
 - 4-Group RMON (RFC1757)

The SNMP Configuration submenu has four options:

- SNMP Configuration
- Trap Configuration
- Individual Trap Configuration
- Quit to previous menu

A terminal window titled "Terminal — telnet — 80x24" showing the configuration menu for an IC3624PWR Remote Management System. The menu is titled "Basic Switch Configuration -> SNMP Configuration Menu" and lists four options: "SNMP [M]anagement Configuration", "SNMP [T]rap Receiver Configuration", and "[Q]uit to previous menu". A "Command>" prompt is visible at the bottom left. A black banner at the bottom of the terminal window contains the text "Enter the character in square brackets to select option".

```
Terminal — telnet — 80x24
IC3624PWR Remote Management System
Basic Switch Configuration -> SNMP Configuration Menu

SNMP [M]anagement Configuration
SNMP [T]rap Receiver Configuration
[Q]uit to previous menu

Command> 
Enter the character in square brackets to select option
```

6.2.3.1 SNMP Management Configuration

The SNMP Configuration screen lists all SNMP managers and associated information. There are two default community strings, private and public. Read-only is allowed with public mode and read-write is allowed in private mode. You can change the community strings to meet your network requirements.

Map: Main Menu->Basic Configuration Menu->SNMP Configuration->SNMP Management Configuration

```

Terminal - telnet - 80x24
IC3624PWR Remote Management System
SNMP Configuration -> SNMP Management Configuration Menu

SNMP Manager List:
No.   Status   Privilege   IP Address   Community
-----
1     Enabled  Read-Write  0.0.0.0     private
2     Enabled  Read-Only   0.0.0.0     public
3     Disabled Read-Only   0.0.0.0
4     Disabled Read-Only   0.0.0.0
5     Disabled Read-Only   0.0.0.0
6     Disabled Read-Only   0.0.0.0
7     Disabled Read-Only   0.0.0.0
8     Disabled Read-Only   0.0.0.0
9     Disabled Read-Only   0.0.0.0
10    Disabled Read-Only   0.0.0.0

----- <COMMAND> -----

Set Manager [S]tatus      Set Manager [I]P          [Q]uit to previous menu
Set Manager P[r]ivilege  Set Manager [C]ommunity

Command> 
Enter the character in square brackets to select option

```

The following table describes the four commands used to set the Manager IP, Community string, Status and Privilege.

| | |
|------------------------|---|
| Set Manager Status: | Enable or disable a community string. |
| Set Manager Privilege: | Set the access privilege, 1 is Read-only and 2 is Read-Write. |
| Set Manager IP: | Set the IP address of a specified community. The access is restricted to specified IP only. |
| Set Manager Community: | Set community string. |

6.2.3.2 Trap Configuration

All hosts in community strings with TRAP privileges are notified when a trap condition occurs.

Map: Main Menu->Basic Configuration Menu->SNMP Configuration->Trap Configuration

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
SNMP Configuration -> SNMP Trap Receiver Configuration Menu

Trap Receiver List:
No.   Status   Type   IP Address   Community
-----
1     Disabled v1     0.0.0.0
2     Disabled v1     0.0.0.0
3     Disabled v1     0.0.0.0
4     Disabled v1     0.0.0.0
5     Disabled v1     0.0.0.0
6     Disabled v1     0.0.0.0
7     Disabled v1     0.0.0.0
8     Disabled v1     0.0.0.0
9     Disabled v1     0.0.0.0
10    Disabled v1     0.0.0.0

----- <COMMAND> -----

Set Receiver [S]tatus  Set Receiver [I]P      In[d]ividual Trap Config
Set Trap [T]ype       Set Receiver [C]ommunity [Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

6.2.3.3 Individual Trap Configuration

When this feature is enabled the system generates an SNMP trap when a host authorization failure occurs. The failure occurs when a host tries to gain access to the system and the host's IP address is not in the SNMP host table.

Map: Main Menu->Basic Configuration Menu->SNMP Configuration->Trap Receiver Configuration

SNMP Authentication Failure Trap

| | |
|---------|--|
| Enable | The system will generate a SNMP trap upon a host authorization failure |
| Disable | The authentication traps will not be generated |

All hosts in community strings with TRAP privileges are notified when a trap condition occurs. Three commands used to set the trap condition are as follows:

| | |
|--------------------------------|--|
| Enable/Disable Auth Fail Trap: | Enable or disable the authentication failure trap. |
| Add Link Down Trap Ports: | Add individual port onto the trap list. |
| Delete Link Down Trap Ports: | Delete individual port from the trap list |

Port Link Down Trap

When this feature is enabled, the system generates an SNMP trap upon a port link down. The failure occurs when a link is disconnected. You can enable or disable each port independently.

| | |
|---------|--|
| Enable | The system generates a SNMP trap upon a port link down |
| Disable | The port link down trap is not generated upon a port link down |

As authentication failure trap, all hosts in community strings with TRAP privileges are notified when a trap condition occurs.

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
SNMP Trap Receiver Configuration -> Enable/Disable Individual Trap Menu

SNMP Authentication Failure : Disabled
Enable Link Up/Down Port: 1-26
PoE Trap Control: Enabled

----- <COMMAND> -----

Enable/Disable [A]uth Fail Trap
Add Link Up/Down Trap [P]orts
[D]elete Link Up/Down Trap Ports
Enable/Disable Po[E] Trap
[Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

There are five submenus available from this screen Community string, Status and Privilege.

- Enable/Disable Authorization Fail Trap
- Add Link Up/Down Trap Ports
- Delete Link Up/Down Trap Ports
- Enable/ Disable PoE Trap
- Quit to previous menu

6.2.4 Port Configuration

In the Basic Port Configuration menu, you can set the port admin status, mode, and flow control. The following is an example from the GUI interface.

Map: Main Menu->Basic Configuration Menu->Port Configuration

The screenshot displays the ASANTE network switch GUI. On the left is a navigation sidebar with options like General Info, Basic Config, Admin. Config, IP Config, SNMP Config, Port Config, System Security C., Username/Password, Forwarding DB, SMTP Config, ARP Table, Advanced Config, and Tools. The main content area is titled 'Port Configuration'. It features a 'Port Index' row with 26 ports and 'Set All' and 'Clear All' buttons. Below this is a configuration table with columns for Admin Status, Mode, and Flow Ctl, each with a dropdown menu and an 'Apply' button. A note states: 'Note: Giga ports can be config to 1000 Fdx only if port 25 or port 26 be checked'. At the bottom is a detailed table for ports 1-10:

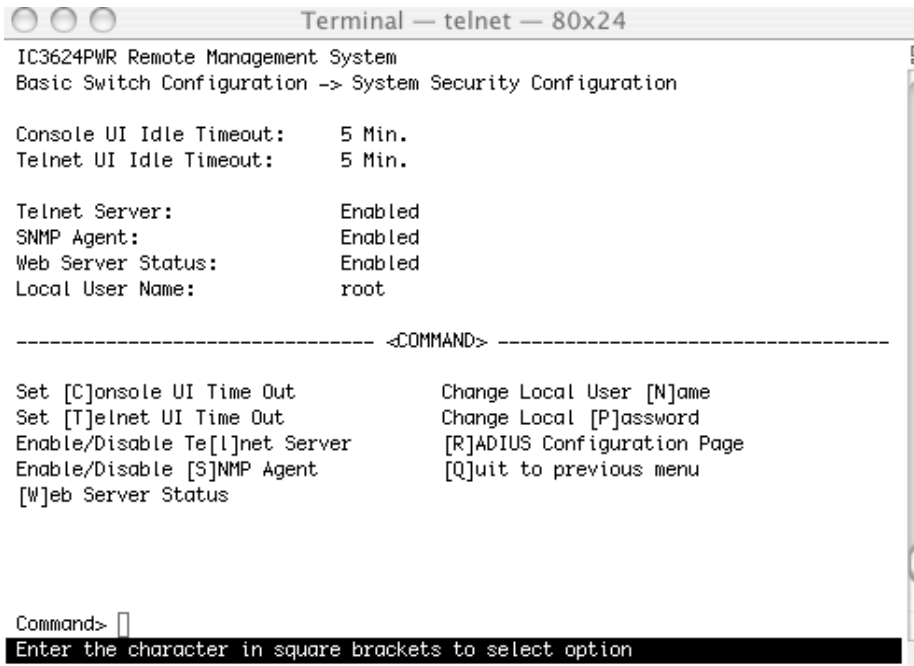
| Port Index | Trunk | Type | Admin Status | Link Status | Mode | Flow Ctl |
|------------|-------|-------|--------------|-------------|------|----------|
| 1 | --- | 100TX | Enabled | Down | Auto | Disabled |
| 2 | --- | 100TX | Enabled | Down | Auto | Disabled |
| 3 | --- | 100TX | Enabled | Down | Auto | Disabled |
| 4 | --- | 100TX | Enabled | Down | Auto | Disabled |
| 5 | --- | 100TX | Enabled | Down | Auto | Disabled |
| 6 | --- | 100TX | Enabled | Down | Auto | Disabled |
| 7 | --- | 100TX | Enabled | Down | Auto | Disabled |
| 8 | --- | 100TX | Enabled | Down | Auto | Disabled |
| 9 | --- | 100TX | Enabled | Down | Auto | Disabled |
| 10 | --- | 100TX | Enabled | Down | Auto | Disabled |

6.2.5 System Security

This screen allows you to enable or disable the web, SNMP, and/or telnet interfaces, as well as change the user name and password. User names and passwords are case sensitive and can be up to 12 characters long.

Map: Main Menu->Basic Configuration Menu->System Security

| | |
|-------------------------------|--|
| Set Console UI Time Out: | The session is disconnected when the time out occurs |
| Set Telnet UI Time Out: | The telnet session is disconnected when the time out occurs. |
| Change Local User Name: | Change the name of local user |
| Change Local Password: | Change the password of local user |
| Enable/Disable Telnet Server: | Enable or disable the system accessibility using telnet. |
| Enable/Disable SNMP Agent: | Enable or disable the system accessibility using SNMP |
| Enable/Disable Web Server: | Enable or disable the system accessibility using web browser |



```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Basic Switch Configuration -> System Security Configuration

Console UI Idle Timeout:      5 Min.
Telnet UI Idle Timeout:      5 Min.

Telnet Server:                Enabled
SNMP Agent:                   Enabled
Web Server Status:           Enabled
Local User Name:              root

-----<COMMAND>-----

Set [C]onsole UI Time Out      Change Local User [N]ame
Set [T]elnet UI Time Out      Change Local [P]assword
Enable/Disable Te[l]net Server [R]ADIUS Configuration Page
Enable/Disable [S]NMP Agent    [Q]uit to previous menu
[W]eb Server Status

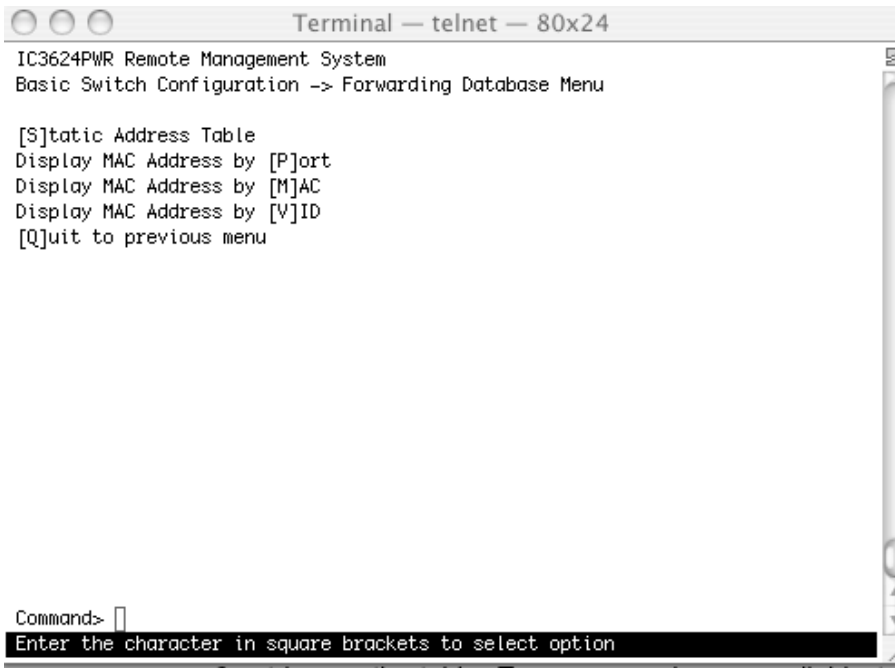
Command> 
Enter the character in square brackets to select option

```

6.2.6 Forwarding DB

Use the Forwarding Database menu to view the dynamic MAC addresses in the address database. When addresses are in the database, the packets are forwarded directly to the specified ports. You can display addresses in the table by port, VLAN, or MAC address. Use the Static Addresses Table to specify Media Access Control (MAC) addresses for specific ports that you do not want to be purged from the table by the aging function.

Map: Main Menu->Basic Configuration Menu->Forwarding DB



```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Basic Switch Configuration -> Forwarding Database Menu

[S]tatic Address Table
Display MAC Address by [P]ort
Display MAC Address by [M]AC
Display MAC Address by [V]ID
[Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

There are four commands available on this menu.

| | |
|-----------------------------|---|
| Static Address Table | Display and configure the static MAC address table. |
| Display MAC Address By Port | Display MAC address table for a specified port |
| Display MAC Address by MAC | Display MAC address in order of MAC address. |
| Display MAC Address by VID | Display MAC address table for a specified VLAN ID. |

The following figures show an instance of Static Address Table. There are 3 entries on the table. Two commands are available to add or remove an entry. The following is an example of adding an entry:

```
Enter MAC Address(xx:xx:xx:xx:xx:xx) > 00:12:34:99:ab:ef <ENTER>
Add new entry->Enter port number > 10 <ENTER>
Add new entry->Enter VLAN ID> 50 <ENTER>
```

A new entry appears:

```
00:12:34:99:AB:EF    10    50
```

The following is an example of removing an entry:

```
Hit key D
Enter MAC Address(xx:xx:xx:xx:xx:xx) > 00:11:ab:00:33:55 <ENTER>
Delete entry->Enter VLAN ID> 30 <ENTER>

Display MAC Address by Port, MAC, and VID
```

As the number of hosts increase on a network, the Forwarding Database increases. You can view the MAC addresses: by a specified port, sorted by MAC address, or by a specified VLAN. Each one of these has a specified Age-Out time command to remove a non-recently-used entry. The modification of this timer affects the entire switch.

The age-out time is the amount of time that an entry stays in the bridge table. The range is between 10 seconds and 1,000,000 seconds. The default is 300 seconds.

6.2.7 SNTP Configuration

Depending on the business model, Simple Network Time Protocol (SNTP) synchronizes the network and the services provided. You determine network performance according to the types of services needed by network management systems and engineering resources.

There are four commands on this menu. The example below is from the GUI interface.

Map: Main Menu->Basic Configuration Menu->SNTP Configuration

| | |
|---------------------|--|
| Set SNTP Server IP | Use to set Simple Network Time Protocol, enter SNTP server IP to get into it |
| Set SNTP Interval | Use to set up SNTP polling interval, for example 1min |
| Set Time Zone | Use to set the time zone Pacific |
| Set Daylight Saving | Use to set up the daylight saving |

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Basic Switch Configuration -> SNTP Configuration Menu

Time ( HH:MM:SS ) : 06:09:34
Date ( YYYY/MM/DD ) : 1900/01/01   Thursday

SNTP Server IP      : 0.0.0.0
SNTP Polling Interval : 1 Min
Time Zone : (GMT-08:00) Pacific Time (US & Canada),Tijuana
Daylight Saving      : Disabled

----- <COMMAND> -----

Set SNTP Server I[P]
Set SNTP [I]nterval
Set Time [Z]one
S[e]t Daylight Saving
[Q]uit to previous menu

Command> █
Enter the character in square brackets to select option

```

6.2.8 ARP Table

Use this sub command to set the Address Resolution Protocol (ARP) table timeout, add or modify a static entry and establish the sorting method.

Map: Main Menu->Basic Configuration-> ARP Table

```

Terminal - telnet - 80x24
IC3624PWR Remote Management System
Basic Switch Configuration -> ARP Table

Sorting Method : By IP
ARP Age Timeout : 7200 seconds
  IP Address      Hardware Address  Type
  -----
  69.226.6.78    00:00:89:28:56:72  Dynamic

----- <COMMAND> -----
[N]ext Page                [A]dd/Modify Static Entry
[P]revious Page           [D]elete Entry
Set ARP Age [T]imeout     [Q]uit to previous menu
[S]orting Entry Method
Command> 
Enter the character in square brackets to select option

```

6.3 Advanced Switch Configuration

The Advanced Switch Configuration screen allows you to configure several advanced system-related settings.

Map: Main Menu->Advanced Switch Configuration

There are ten submenus on the Advanced Switch Configuration screen.

- VLAN Management
- Link Aggregation
- Port Monitoring Configuration
- Multiple Spanning Tree Configuration
- Access List Configuration
- Quality of Service Configuration
- Storm Control Configuration
- 802.1 Port Based Access Control Configuration
- SNMP Snooping Configuration
- Power Over Ethernet Configuration

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Main Menu -> Advanced Switch Configuration Menu

[V]LAN Management
[L]ink Aggregation
Port [M]onitoring Configuration
Multiple [S]panning Tree Configuration
Quality of Service [C]onfiguration
St[O]rm Control Configuration
802.1[X] Port Based Access Control Configuration
[I]GMP Snooping Configuration
[P]ower Over Ethernet Configuration
[Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

6.3.1 VLAN Management

A virtual LAN (VLAN) is a switched network that is segmented by function, project team or application, without regard to the physical locations of the users. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded only to stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN are forwarded.

Map: Main Menu->Advanced Switch Configuration->VLAN Management

There are three options available on the VLAN Management screen.

- VLAN Table Configuration
- VLAN Port Configuration
- Quit to previous menu

6.3.1.1 VLAN Table Configuration

Use the VLAN Table Configuration screen to create a new VLAN, add new ports to an existing VLAN, remove ports from an existing VLAN, delete a VLAN, set management status or set GVRP status.

Map: Main Menu->Advanced Switch Configuration->VLAN Management

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Advanced Switch Configuration -> VLAN Management Menu

GVRP Status : Enabled                               Total VLANs : 1
VLAN ID  VLAN Name                                VLAN Type  Mgmt
-----  -
      1
      Permanent  UP

----- <COMMAND> -----
[N]ext Page           [C]reate VLAN           [S]et Port Config
[P]revious Page      [D]elete VLAN           Set [G]VRP Status
Set [M]anagement Status C[o]nfig VLAN Member      [Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

The following table describes the six options available from the VLAN Management submenu.

| | |
|----------------------------|--|
| Create VLAN: | Create a new VLAN; a unique ID must be given. |
| Delete VLAN: | Delete a VLAN ID. The entire setup for this VLAN will be erased. |
| Configuration VLAN Member: | Configure the member of a VLAN |
| Set Port Configuration | Set the configuration of a specified port |
| Set GVRP Status: | Enable or disable the GVRP switch-wide. |
| Set Management Status: | Enable or disable the management status of static VLAN. |

Follow these steps to create a new VLAN Group:

1. Select Create VLAN
2. Enter the VLAN ID and name in the appropriate fields
3. Add the VLAN members
4. Click Apply

Follow these steps to delete a VLAN Group:

1. Select Delete VLAN
2. Enter the corresponding VLAN ID

Follow these steps to configure a VLAN member:

1. Select Configuration VLAN Member
2. Give the corresponding VLAN ID
3. Modify the VLAN members
4. Click Apply.

Follow these steps to set GVRP Status:

1. Select Set GVRP Status
2. Choose E to enable and D to disable

Follow these steps set Management Status:

1. Select Set Management Status
2. Choose U to enable and D to disable.

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Advanced Switch Configuration -> VLAN Management Menu

GVRP Status : Enabled                Total VLANs : 1
VLAN ID  VLAN Name                    VLAN Type  Mgmt
-----
1                               Permanent  UP

Enter VLAN ID > [ ]

----- <COMMAND> -----
[N]ext Page           [C]reate VLAN       [S]et Port Config
[P]revious Page      [D]elete VLAN       Set [G]VRP Status
Set [M]anagement Status  C[o]nfig VLAN Member  [Q]uit to previous menu
  
```

VLAN ID is in range from 1 to 4094

6.3.1.2 VLAN Port Configuration

Use this sub menu to individually configure VLAN ports.

Map: Main Menu->Advanced Switch Configuration->VLAN Management->VLAN Port Configuration

Four options are available from the VLAN Port Configuration screen.

- Set Port VID
- Set Frame Type

- Set GVRP Status
- Quit to previous menu

| | |
|------------------|--|
| Set Port VID: | Set PVID of a port. |
| Set Frame Type: | Set the acceptable frame types, All or Tagged Only. When the Tagged Only is selected, all non-tagged packet are dropped. |
| Set GVRP Status: | Enable or disable the GVRP of a port. |

Note: When you delete an existing PVID the switch uses the default PVID1.

6.3.2 Link Aggregation

The Trunk Configuration screen is used to set multiple links between switches to work as one virtual link (aggregate link). Trunk can only be defined for similar port types. For example, a 10/100 port cannot form a Port Trunk with a gigabit port. For 10/100 ports, Trunk can only be formed within the same bank. A bank is a set of eight ports. Up to four Trunk can be operating at the same time. Toggle the ports to the correct Trunk number to set up a Trunk. Click Apply to enable the Trunk. Spanning Tree treats the Trunk ports as a single virtual port.

The Port Link Aggregation feature allows multiple links between switches to work as one virtual link or aggregate link. Link Aggregation is only defined for similar port types. For example, a 10/100 port cannot form a Port Link Aggregation with a gigabit port. Spanning Tree treats Link Aggregation ports as a single virtual port.

Map: Main Menu->Advanced Switch Configuration->Link Aggregation

There are seven options available from the Link Aggregation submenu.

- Set System Priority
- Add a Group Member
- Delete a Group Member
- Modify a Group Mode
- Set Port Priority
- LACP Group Status

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Advanced Switch Configuration -> Trunk Configuration Menu
System Priority : 1

Key      Mode      Member Port List
-----
-----

----- <COMMAND> -----
Se[t] System Priority          Set P[ort] Priority
[A]dd Group Member           LACP [G]roup Status
[R]emove Group Member        [Q]uit to previous menu
[M]odify Group Mode
Command> [ ]
Enter the character in square brackets to select option

```

6.3.2.1 Set Port Priority

The default system priority is the same in all ports. To set up a port with a different priority in the link aggregation, use the Set Port Priority.

Map: Main Menu->Advanced Switch Configuration->Trunk Configuration->Set Port Priority

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Advanced Switch Configuration -> Trunk Configuration Menu
System Priority : 1

Key      Mode      Member Port List
-----
-----

----- <COMMAND> -----
Se[t] System Priority          Set P[ort] Priority
[A]dd Group Member           LACP [G]roup Status
[R]emove Group Member        [Q]uit to previous menu
[M]odify Group Mode
Enter system priority for LACP> [ ]
System priority is in range from 0 to 65535

```

6.3.3 Port Monitoring

The Port Monitoring screen is used to designate a port for monitoring traffic from one port configured on the switch. The switch monitors the network activity by copying all traffic from the specified monitoring sources to the designated monitoring port to the attached network analyzer.

Map: Main Menu->Advanced Switch Configuration->Port Monitoring

There are five options available from this menu.

| | |
|---------------------------|--|
| Set Monitoring Port: | Set the monitoring port. All monitored traffic is forwarded to this port |
| Set Port to be Monitored: | Set the monitored port. All traffic through this port is forwarded to the monitoring port |
| Set Traffic Direction: | Set the direction of monitored traffic, receiving(R), transmission (T) or both direction (B) |
| Change Mirror Status: | Enable or disable the mirror status |

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Advanced Switch Configuration -> Port Monitoring Configuration Menu

Monitoring Port   Be Monitored Port   Direction   Status
-----
          1           2           Both         Disabled

----- <COMMAND> -----

[S]et Monitoring Port
Set Port to be [M]onitored
Set Traffic [D]irection
[C]hange Mirror Status
[Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

6.3.4 MSTP Configuration

This switch supports rapid spanning tree (IEEE 802.1w) to reduce time required to establish a tree. Each spanning tree establishment process takes several timeouts in order to avoid looping, even the edge switch. You can configure this switch to avoid the long latency due to timeouts if there is only a single connection to the switch. In case of two or more links to the switch and Rapid Spanning Tree is enabled, the switch may not perform properly.

This switch supports IEEE 802.1s Multiple Spanning Tree (MSTP). An independent spanning tree is established per VLAN.

Map: Main Menu->Advanced Switch Configuration->MST Configuration

There are 11 submenus at MSTP Configuration Menu:

- Global Commands:
- Enable/Disable Global MSTP
- Set MSTP Protocol Version
- Set MSTP Configuration Name
- Set MSTP Revision Level
- CIST Configuration
- CIST Basic Port Config
- CIST Advanced Port Configuration
- MSTP Instance Configuration
- Designated Topology
- Regional Topology
- Quit to previous menu

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Advanced Switch Configuration -> Multiple Spanning Tree Configuration

Global MSTP Status: Disabled
Protocol Version      : MSTP
MST Configuration Name : 00:30:ab:25:8c:31
MST Revision Level    : 0
MST Config Digest     : ac36177f50283cd4b83821d8ab26de62

----- <COMMAND> -----

[E]nable/Disable Global MSTP      CIST [B]asic Port Configuration
Set MSTP Protocol [V]ersion       CIST [A]dvanced Port Configuration
Set MSTI Configuration [N]ame     MSTP Ins[t]ance Configuration
Set MSTI [R]evision Level         Designated Topology [I]nformation
CIST [C]onfiguration              Re[g]ional Topology Information
                                   [Q]uit to previous menu

Command> █
Enter the character in square brackets to select option

```


The following tables define the global information that is access and configure through this submenu.

| | |
|-------------------------|--|
| Global MSTP Status: | The status of global multiple spanning tree protocol. Enable indicates that MSTP is running. Disable indicates that MSTP is not running. |
| Protocol Version: | The protocol can be one of three versions, SPT (Spanning Tree), RSPT (Rapid Spanning Tree), and MSTP (Multiple Spanning Tree). |
| MST Configuration Name: | The name of MSPT region, this must be identical to other switches in order to have VLAN work cross-switch. |
| MST Revision Level: | The version of MSPT region, this must be identical to other switches in order to have VLAN work cross-switch. |
| MST Config Digest: | The digest value of configuration data to increase the security. |

Commands

| | |
|------------------------------|--|
| Enable/Disable Global MSTP | Enables or disables the switch-wide MSTP. |
| Set MSTP Protocol Version: | Sets the protocol as SPT (Spanning Tree), RSPT (Rapid Spanning Tree) and MSPT (Multiple Spanning Tree) |
| Set MSTP Configuration Name: | Sets the configuration name |
| Set MSTP Revision Level: | Sets the revision level |

The Common Instant Spanning Tree Configuration Menu allows you to configure the switch-wide parameters, such as Cist Hello Time, Cist Maximum Age, Cist Forward Delay, and so on.

6.3.4.1 CIST Configuration

Use this submenu to configure the Common Internal Spanning Tree (CIST).

Map: Main Menu->Advanced Switch Configuration->MSTP Configuration->CIST Configuration

Status

| | |
|------------------|---|
| Hello Time: | Amount of time between configuration messages sent by the Spanning Tree algorithm |
| Maximum Age | Amount of time before a configuration message is discarded by the system |
| Forward Delay | Amount of time system spent transitioning from the 'learning' to the 'listening' to the 'forwarding' states |
| Bridge Priority | Priority setting among other switches in the Spanning Tree |
| Cost & Priority: | Refer to the following table for complete information |

| Parameters | Range | Description |
|-----------------|-------------|--|
| PrtY (Priority) | 0-240 | STP uses this to determine which path (port) to use for forwarding. The port with the lowest number has the highest priority. |
| Cost | 0-200000000 | The switch uses this to determine which port is the forwarding port when the priority is equal. The path with the lowest cost to the root bridge is the active path. The estimated path cost is the industry standard for the port speed. The default path cost is the maximum speed for the port. |

Commands

| | |
|-------------------------------|--|
| Set Cist Bridge Priority: | Sets the Cist bridge priority. |
| Set Cist Bridge Hello Time: | Sets the interval between two hello packets. |
| Set Cist Bridge Maximum Age: | Sets the maximum age time. |
| Set Cist bridge Forward Delay | Sets the forward delay. |
| Set MSTP Max Hop Count Delay: | Sets the maximum hop count delay. |

Rapid Spanning Tree

When a port running the standard STP is connected, it goes through the STP negotiation (listening -> learning -> forwarding or blocking) before it is available. If a client is trying to access a server through the switch running the STP negotiation, it cannot connect to it immediately. RSPT solves the lag time issue by setting the port directly to forwarding mode, which allows any server access request to be forwarded. RSPT is used on end node ports. For example, ports connected to PCs or servers, and not on uplink ports to other switches.

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Multiple Spanning Tree Configuration -> CIST Configuration

CIST Root Port:      0          Time Since Topology Change: 0      Sec.
CIST Root Path Cost: 0          Topology Change Count:      0
CIST Root:           0000 000000000000
CIST Regional Root Cost: 0      CIST Bridge ID:           0000 000000000000
CIST Regional Root: 0000 000000000000 CIST Bridge Hello Time: 2      Sec.
CIST Bridge Maximum Age: 20     Sec.
CIST Hello Time:     2          Sec.      CIST Bridge Forward Delay: 15   Sec.
CIST Maximum Age:   20         Sec.      Max Hop Count:             20
CIST Forward Delay: 15         Sec.

----- <COMMAND> -----

Set CIST Bridge [P]riority          Set CIST Bridge [F]orward Delay
Set CIST Bridge [H]ello Time       Set MSTP Max H[o]p Count
Set CIST Bridge [M]aximum Age      [Q]uit to previous menu

Command> [ ]
Enter the character in square brackets to select option

```

6.3.4.2 CIST Basic Port Configuration

Set the port priority, the path cost for each port and enable or disable the port STP status to increase the network efficiency.

Map: Main Menu->Advanced Switch Configuration->MSTP Configuration->CIST Configuration

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Multiple Spanning Tree Configuration -> CIST Basic Port Configuration

Port  Trunk  Link   State   Role   Priority  Path Cost  STP Status
----  ----  ----  -
1     ---     Down  Forwarding Disabled 128    200000(A) Enabled
2     ---     Down  Forwarding Disabled 128    200000(A) Enabled
3     ---     Down  Forwarding Disabled 128    200000(A) Enabled
4     ---     Down  Forwarding Disabled 128    200000(A) Enabled
5     ---     Down  Forwarding Disabled 128    200000(A) Enabled
6     ---     Down  Forwarding Disabled 128    200000(A) Enabled
7     ---     Up    Forwarding Disabled 128    200000(A) Enabled
8     ---     Down  Forwarding Disabled 128    200000(A) Enabled
9     ---     Down  Forwarding Disabled 128    200000(A) Enabled
10    ---     Down  Forwarding Disabled 128    200000(A) Enabled
11    ---     Down  Forwarding Disabled 128    200000(A) Enabled
12    ---     Down  Forwarding Disabled 128    200000(A) Enabled

----- <COMMAND> -----

[N]ext Page          Set Port Path [C]ost
[P]revious Page     Set Port STP [S]tatus
Set Port Pr[i]ority [Q]uit to previous menu

Command> [ ]
Enter the character in square brackets to select option

```

6.3.4.3 Advanced CIST Port Configuration

Set the port edge status, the port-to-port status, and restart port migration to prevent the wrong link.

Map: Main Menu->Advanced Switch Configuration->MSTP Configuration->CIST Configuration

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Multiple Spanning Tree Configuration -> CIST Advanced Port Configuration

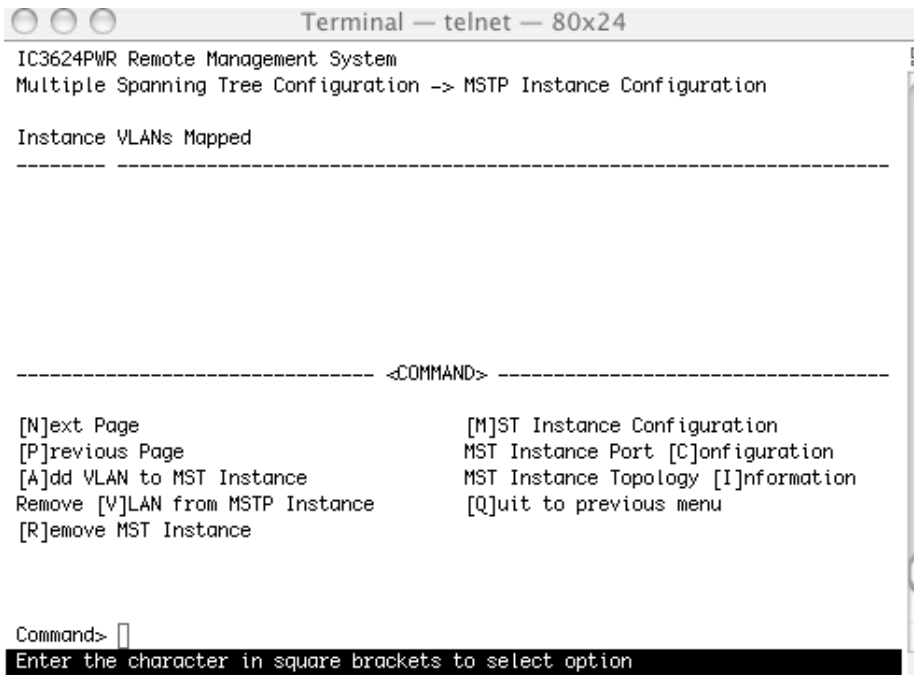
Port Trunk  Link   State   Role   Admin/OperEdge  Admin/OperPtoP  Migrat
-----
 1 --- Down Forwarding Disabled  False/False    Auto /False    Init.
 2 --- Down Forwarding Disabled  False/False    Auto /False    Init.
 3 --- Down Forwarding Disabled  False/False    Auto /False    Init.
 4 --- Down Forwarding Disabled  False/False    Auto /False    Init.
 5 --- Down Forwarding Disabled  False/False    Auto /False    Init.
 6 --- Down Forwarding Disabled  False/False    Auto /False    Init.
 7 --- Up   Forwarding Disabled  False/False    Auto /False    Init.
 8 --- Down Forwarding Disabled  False/False    Auto /False    Init.
 9 --- Down Forwarding Disabled  False/False    Auto /False    Init.
10 --- Down Forwarding Disabled  False/False    Auto /False    Init.
11 --- Down Forwarding Disabled  False/False    Auto /False    Init.
12 --- Down Forwarding Disabled  False/False    Auto /False    Init.
-----<COMMAND>-----
[N]ext Page           Set Port P-[t]o-P Status
[P]revious Page      Restart Port [M]igration
Set Port [E]dge Status  [Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

6.3.4.4 MSTP Instance Configuration

Use the MSTP Instance Configuration screen when configuring a small tree in the MSTP. One Instance can have more than one VLAN. In this page, you can add, remove VLAN or remove, for the MST Instance and Instance Port configuration.

Map: Main Menu->Advanced Switch Configuration->MSTP Configuration->MSTP Instance Configuration

```
Terminal — telnet — 80x24
IC3624PWR Remote Management System
Multiple Spanning Tree Configuration -> MSTP Instance Configuration

Instance VLANs Mapped
-----

-----<COMMAND>-----

[N]ext Page                [M]ST Instance Configuration
[P]revious Page           MST Instance Port [C]onfiguration
[A]dd VLAN to MST Instance MST Instance Topology [I]nformation
Remove [V]LAN from MSTP Instance [Q]uit to previous menu
[R]emove MST Instance

Command> 
Enter the character in square brackets to select option
```

6.3.4.5 Designated Topology Information

Use this screen to view topology information, the status of the links and designated root, bridge and port numbers.

Map: Main Menu->Advanced Switch Configuration->MSTP Configuration->Designated Topology Information

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Multiple Spanning Tree Configuration -> Designated Topology Information

Port Trunk Link Cist Cist Cist Cist
  --- --- --- Desig. Root Desig. Cost Desig. Bridge Desig. Port
-----
1 --- Down 8000 0030ab258c31 0 8000 0030ab258c31 00 01
2 --- Up 8000 0030ab258c31 0 8000 0030ab258c31 00 02
3 --- Down 8000 0030ab258c31 0 8000 0030ab258c31 00 03
4 --- Down 8000 0030ab258c31 0 8000 0030ab258c31 00 04
5 --- Down 8000 0030ab258c31 0 8000 0030ab258c31 00 05
6 --- Down 8000 0030ab258c31 0 8000 0030ab258c31 00 06
7 --- Up 8000 0030ab258c31 0 8000 0030ab258c31 00 07
8 --- Down 8000 0030ab258c31 0 8000 0030ab258c31 00 08
9 --- Down 8000 0030ab258c31 0 8000 0030ab258c31 00 09
10 --- Down 8000 0030ab258c31 0 8000 0030ab258c31 00 0a
11 --- Down 8000 0030ab258c31 0 8000 0030ab258c31 00 0b
12 --- Down 8000 0030ab258c31 0 8000 0030ab258c31 00 0c
-----
<COMMAND>
-----

[N]ext Page [P]revious Page [Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

6.3.4.6 Regional Topology Information

This page shows regional topology information.

Map: Main Menu->Advanced Switch Configuration->MSTP Configuration->Regional Topology Information

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Multiple Spanning Tree Configuration -> Regional Topology Information

Port Trunk Link Cist Port Regional Root Cist Port Regional Path Cost
-----
1 --- Down 8000 0030ab258c31 0
2 --- Up 8000 0030ab258c31 0
3 --- Down 8000 0030ab258c31 0
4 --- Down 8000 0030ab258c31 0
5 --- Down 8000 0030ab258c31 0
6 --- Down 8000 0030ab258c31 0
7 --- Up 8000 0030ab258c31 0
8 --- Down 8000 0030ab258c31 0
9 --- Down 8000 0030ab258c31 0
10 --- Down 8000 0030ab258c31 0
11 --- Down 8000 0030ab258c31 0
12 --- Down 8000 0030ab258c31 0
-----
<COMMAND> -----

[N]ext Page [P]revious Page [Q]uit to previous menu

Command> [ ]
Enter the character in square brackets to select option

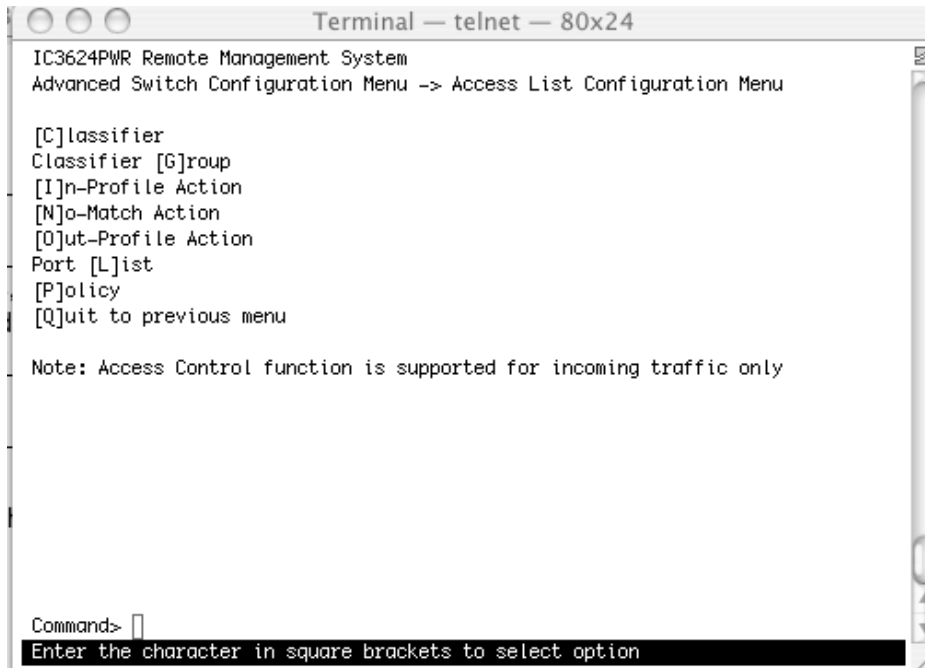
```

6.3.5 Access List Configuration

There are seven functions for access control.

Map: Main Menu->Advanced Switch Configuration->Access List Configuration

| | |
|--------------------|--|
| Classifier | Classifier selects packets stream based on the value of combination of one or more header fields such as source IP address, destination IP address, DS field, protocol ID, source port and destination port numbers, and others. |
| Classifier Group | A show group status and allows you to join, remove and set group names. |
| In-Profile Action | According to traffic profile specification, packets in the traffic stream arrive when tokens are available in the bucket. It takes action specified in in-profile action if traffic stream match in-profile. |
| No-Match Action | If a classifier were based on one or more header fields that did not select packets, it would take action specified in No-Match action. |
| Out-Profile Action | Packets in traffic stream arrive when insufficient tokens are available in the bucket take action specified in out-profile action if traffic stream match out-profile. |
| Port List | An ingress port handling traffic as it enters one or more ports. |
| Policy | A policy consists of classifier, precedence port list, in /out profile or no match action. When packets enter, a DS domain traffic flow should be conditioned at the DS ingress node of the DS domain according to the appropriate policy. |

A terminal window titled "Terminal — telnet — 80x24" displays the configuration menu for an IC3624PWR Remote Management System. The menu is titled "Advanced Switch Configuration Menu -> Access List Configuration Menu" and lists several options in square brackets: [C]lassifier, [G]roup, [I]n-Profile Action, [N]o-Match Action, [O]ut-Profile Action, [L]ist, [P]olicy, and [Q]uit to previous menu. A note below the menu states: "Note: Access Control function is supported for incoming traffic only". At the bottom, a "Command>" prompt is followed by a cursor and a black bar containing the instruction "Enter the character in square brackets to select option".

```
Terminal — telnet — 80x24
IC3624PWR Remote Management System
Advanced Switch Configuration Menu -> Access List Configuration Menu

[C]lassifier
[G]roup
[I]n-Profile Action
[N]o-Match Action
[O]ut-Profile Action
[L]ist
[P]olicy
[Q]uit to previous menu

Note: Access Control function is supported for incoming traffic only

Command> 
Enter the character in square brackets to select option
```

6.3.5.1 Classifier Configuration Menu

Use this submenu to create, delete and modify classifier fields.

Map: Main Menu->Advanced Switch Configuration->Access Control->Classifier Configuration Menu

Three commands are available in this screen.

- Create Classifier
- Delete Classifier
- Modify Classifier
- Classifier

The following describes the classifier fields.

| | |
|-------------------------------------|---|
| Source IP address: | Selected packets depend on source IP address |
| Source IP address mask length: | Selected packets depend on one domain or single host |
| Destination IP address: | Selected packets depend on destination IP address |
| Destination IP address mask length: | Selected packets depend on one domain or single host |
| DSCP: | Selected packets depend on DS code point value range from 0 to 63 |
| Protocol: | Selected packets depend on protocol range from 1 to 255 |
| Source layer 4 port: | Selected packets depend on source port number specified in TCP header field range from 1-65535 |
| Destination layer 4 port: | Selected packets depend on destination port number specified in TCP header field range from 1-65535 |
| Source MAC address: | Selected packets depend on source MAC address specified in Ethernet header source MAC field |
| Destination MAC address: | Selected packets depend on destination MAC address specified in Ethernet header destination MAC field |
| VLAN ID: | Selected packets depend on VLAN ID value specified in Ethernet header VID field |

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Access List Configuration -> Classifier Configuration Menu
Multifield Classifier:                               Total Entries : 0
Index  Src IP Addr  Dst IP Addr  DSCP  Protocol  Src L4 Port  Dst L4 Port
-----
-----

----- <COMMAND> -----
[N]ext Page           M[o]dify Classifier           [J]oin Classifier Group
[P]revious Page      [M]ore Classifier Info...     [Q]uit to previous menu
[C]reate Classifier   [S]how Detailed Entry Info.
[D]elete Classifier
Command> [ ]
Enter the character in square brackets to select option

```

6.3.5.2 Classifier Group

Use this submenu to create or delete classifiers, join classifiers, remove, classifiers, set classifier group names.

6.3.5.3 In Profile Action

From this screen you can create, delete, and modify the action for the different in-bound profiles.

Map: Main Menu->Advanced Switch Configuration->Access Control->In Profile Action

Three options are available from the In-Profile Action submenu.

- Create In-Profile Action
- Delete In-Profile Action
- Modify In-Profile Action
- In Profile Action

There are four options available when using the In-profile action menu:

| | |
|---------------------|---|
| Drop: | Shows the number of dropped packets |
| Policed-dscp: | Changes TOS -DS (first 6 bits) field value |
| Policed-precedence: | Changes TOS-precedence (first 3 bits) field value |
| Policed-cos: | Changes 802.1p value within TAG filed used to determined hardware CoS queue |

```

Terminal - telnet - 80x24
IC3624PWR Remote Management System
Access List Configuration -> In-Profile Action Configuration Menu
In-Profile Action:      Total Entries : 0
Index  Deny/Permit/Pass  Policed-DSCP  Policed-Precedence  Policed-CoS
-----
-----

----- <COMMAND> -----
[N]ext Page              [D]elete In-Profile Action
[P]revious Page         [M]odify In-Profile Action
[C]reate In-Profile Action  [Q]uit to previous menu
Command> 
Enter the character in square brackets to select option

```

6.3.5.4 No Match Action

From this screen you can create, delete, and modify the action for the different actions where there is no match.

Map: Main Menu->Advanced Switch Configuration->Access Control->No Match Action

Three options are available from this screen.

- Create No-Match Action
- Delete No-Match Action
- Modify No-Match Action
- No-Match Action is the same as In-Profile Action. No-match action only supports 81 entries.

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Access List Configuration -> No-Match Action Configuration Menu
No-Match Action:      Total Entries : 0
Index  Deny/Pass  Policed-DSCP  Policed-Precedence  Policed-CoS
-----
-----

----- <COMMAND> -----
[N]ext Page           [D]elete No-Match Action
[P]revious Page      [M]odify No-Match Action
[C]reate No-Match Action  [Q]uit to previous menu
Command> 
Enter the character in square brackets to select option

```

6.3.5.5 Out Profile Action

From this screen you can create, delete, and modify the action for the different out-bound profiles.

Map: Main Menu->Advanced Switch Configuration->Access Control->Out Profile Action

Three options are available in this menu.

- Create Out-Profile Action
- Delete Out-Profile Action
- Modify Out-Profile Action
- Out Profile Action

| | |
|-----------------|---|
| Drop: | Number of dropped packets |
| Policed-dscp: | Changes TOS-DS (first 6 bits) field |
| Committed rate: | Configures committed rate to determine how traffic flow is allowed to pass. The packet is considered in-profile if it conforms to the bandwidth profile, out-profile otherwise. |
| Burst size: | Sets the burst size of a full bucket. When the token level is below the threshold value this indicates there is no available bandwidth (Note: Threshold value is 2KB) |

6.3.5.6 Port List

From this screen you can create, delete, and modify the action for the different port lists.

Map: Main Menu->Advanced Switch Configuration->Access Control->Port List

An ingress port in its role in handling traffic as it enters one or more ports you want to do differentiated service.

Three options are available from this screen.

- Create Port List
- Delete Port List
- Modify Port List

```

Terminal - telnet - 80x24
IC3624PWR Remote Management System
Access List Configuration -> Port List Configuration Menu
Port List:          Total Entries : 0
Index      Port List
-----
-----

-----<COMMAND>-----
[N]ext Page          [D]elete Port List
[P]revious Page     [M]odify Port List
[C]reate Port List  [Q]uit to previous menu
Command> [ ]
Enter the character in square brackets to select option

```

6.3.5.7 Policy

Use this submenu to create, delete, enable or disable, show status or sequence and update the policies for the different ports. A policy may associated with classifier, in-profile, no-match, out-profile, port list, and sequence. Classifier and port list are necessary for a policy.

Map: Main Menu->Advanced Switch Configuration->Access Control->Policy

Six options are available in this page:

- Create Policy
- Delete Policy
- Enable or Disable Policy
- Show Policy Entry
- Update Policy
- Display Sequence By Port

6.3.6 Quality of Service Configuration

The priority tag of each packet is divided into four queues on each output port. The default is each queue takes two priorities sequentially. The Administrator may configure the traffic class. The Quality of Service (QoS) only works after the QoS status is enabled. Use the Set QoS Status options to enable this feature.

Map: Main Menu->Advanced Switch Configuration->Quality of Service Configuration

There are two features your can configure from this menu.

- Mapping Method
- Scheduling Method

6.3.6.1 Mapping Method

Use this submenu to set the traffic class mapping method.

Map: Main Menu->Advanced Switch Configuration->Quality of Service Configuration->Mapping Method

The following three functions are available from this screen.

- QoS Status
- Traffic Class Mapping
- Scheduling Method Configuration

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Quality of Service Configuration -> Traffic Class Configuration Menu

QoS Status: Disabled

Priority   Traffic Class
-----
  0         0
  1         0
  2         1
  3         1
  4         2
  5         2
  6         3
  7         3
                                0: Lowest
                                3: Highest

----- <COMMAND> -----

[S]et QoS status                [Q]uit to previous menu
Set Priority-Traffic Class [M]apping
Scheduling Method [C]onfig.

Command> 
Enter the character in square brackets to select option

```

6.3.6.2 Scheduling Method

Use this submenu to set the QoS scheduling method and the traffic class-weight mapping.

Map: Main Menu->Advanced Switch Configuration->Quality of Service Configuration->Scheduling Method

6.3.7 Storm Control

Storm control protects connected Ethernet ports by controlling traffic rates during periods of high volume. When the local device detects excessive traffic at its end, it can notify the link or the remote device by sending a pause frame. The remote device stops sending data packets, which prevents any loss of data packets during the congestion period.

Map: Main Menu->Advanced Switch Configuration->Storm Control

There are three types of storm control settings used to enable, disable and set the threshold value to control the network traffic.

- DLF
- Broadcast
- Multicast


```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Advanced Switch Configuration -> Storm Control Configuration Menu

Global Storm Control Setting:
  DLF      Broadcast  Multicast  Threshold
-----
Disabled   Disabled    Disabled    0

----- <COMMAND> -----
Set [D]LF Status      Set [B]roadcast Status  Set [M]ulticast Status
Set [T]hreshold Value [Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

6.3.8 802.1 Port Based Access Control

Use this menu to view status of the ports and to set port specific values

Map: Main Menu->Advanced Switch Configuration->802.1 Port Based Access Control Configuration

Use this menu to set 13 functions.

- NAS ID
- Port Number
- Port Control
- Port Control Direction
- Transmission Period
- Supplicant Timeout
- Server Timeout
- Maximum Request
- Quiet Period
- Reauthorization Period
- Reauthorization Status
- Initialize
- Reauthorize Initialization

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Advanced Switch Configuration -> Port Based Access Control Configuration Menu

NAS ID                : Nas1
Port No               : 1
Port Status           : Authorized
Port Control          : Force Authorized
Operational Control Direction : Both
Administrative Control Direction: Both
Transmission Period   : 30 seconds
Supplicant Timeout    : 30 seconds
Server Timeout        : 60 seconds
Maximum Request       : 2
Quiet Period          : 60 seconds
Re-authentication Period : 3600 seconds
Re-authentication Status : Disabled
-----<COMMAND>-----
[N]AS ID                Supp[I]licant Timeout    Re-[a]uth Status
[P]ort No               Server Time[o]ut          [I]nitialize
Port [C]ontrol          [M]aximum Request        [R]e-auth Initialize
Port Ctrl [D]irection  Q[u]iet Period           [Q]uit to previous menu
[T]ransmission Period  R[e]-auth Period
Command> [ ]
Enter the character in square brackets to select option

```

6.3.9 IGMP Snooping

In networks where multimedia applications generate multicast traffic, Internet Group Multicast Protocol (IGMP) reduces unnecessary bandwidth usage by limiting traffic forwarding that is normally broadcast throughout network. Enabling IGMP allows individual ports to detect IGMP queries, report packets, and manage IP multicast traffic through the switch.

Map: Main Menu->Advanced Switch Configuration->IGMP Snooping

There are four options available through this menu.

- IGMP Snooping Global Configuration:
- Set IGMP Snooping Status
- Set Host Port Aged Time
- Set Rout Port Aged Time
- Set Report Interval
- Show VLAN Filter Table
- Show Router Port Table
- Quit to previous menu

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Advanced Switch Configuration -> IGMP Snooping Configuration Menu

IGMP Snooping Status      : Disabled
Host Port Age-Out Time    : 260 sec
Router Port Age-Out Time  : 125 sec
Report Forward Interval   : 5 sec
VLAN ID  Group MAC Address  Group Members
-----  -
-----  -

----- <COMMAND> -----
[N]ext Page          Set [H]ost Port Aged Time  Show [V]LAN Filter Table
[P]revious Page     Set [R]outer Port Aged Time Show Router Port [T]able
Set I[G]MP Snooping Status Set Report [I]nterval      [Q]uit to previous menu

Command> [ ]
Enter the character in square brackets to select option

```

You can configure the switch to use Internet Group Management Protocol (IGMP) snooping in subnets that receive IGMP. IGMP snooping constrains multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward multicast traffic only to those ports that want to receive it.

6.3.9.1 Show IGMP Snooping VLAN Filter Table

Set up the VLAN that you do not want to be snooping in the set VLAN Filter Table menu.

Show the results of your configuration using this feature.

Map: Main Menu->Advanced Switch Configuration->IGMP Snooping->Show IGMP Snooping VLAN Filter Table

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
IGMP Snooping Configuration -> Show IGMP Snooping VLAN Filter Table Menu

VLAN ID      Status
-----
-----

----- <COMMAND> -----

[N]ext Page          [S]et VLAN Filter
[P]revious Page     [Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

6.3.9.2 Show Router Port Table

This page shows the ports in some VLANs that are connected to the router. You can snoop the package from router side in these ports.

Map: Main Menu->Advanced Switch Configuration->IGMP Snooping->Show Router Port Table

6.3.10 Power over Ethernet

Power-over-Ethernet (PoE) eliminates the need of 110/220 VAC power source to Wireless Access Points and other devices on a wired LAN. With Power-over-Ethernet system, you need to only run a single CAT5 Ethernet cable that carries both power and data to each device.

Map: Main Menu->Advanced Switch Configuration->Power over Ethernet

There are three submenus.

- PoE Port Configuration
- PoE Global Configuration
- Quit to previous menu

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Advanced Switch Configuration -> Power Over Ethernet Configuration Menu

PoE [P]ort Configuration
PoE [G]lobal Configuration
[Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

6.3.10.1 PoE Port Configuration

Power over Ethernet provides power to connected IEEE 802.3af-compliant powered devices from all 10/100 Ethernet ports if the switch detects that there is no power on the circuit. Use this screen to configure individual ports.

Map: Main Menu->Advanced Switch Configuration->Power Over Ethernet->PoE Port Configuration

Two functions provides for the PoE control.

- Port Configuration
- Global Configuration

6.3.10.1 PoE Port Configuration

| | |
|----------------|--|
| Admin. Status: | The status of administration for a port |
| Priority: | The priority of a PoE port. Three selections are available, critical, high and low. When the power consumption over the power budget, the critical has higher priority on power supplying. |
| Limit(mW): | The maximum power supplied to a port. The default is 15.4W or 15000mW |

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Power Over Ethernet Configuration -> PoE Port Configuration Menu

No. Admin Status      Class Prio. Limit(mW) Pow.(mW) Vol.(V) Cur.(mA)
-----
1  Up  Not Powered    0  Low  15400    0    0    0
2  Up  Powered        2  Low  15400  2013  49.1  41
3  Up  Not Powered    0  Low  15400    0    0    0
4  Up  Not Powered    0  Low  15400    0    0    0
5  Up  Not Powered    0  Low  15400    0    0    0
6  Up  Not Powered    0  Low  15400    0    0    0
7  Up  Not Powered    0  Low  15400    0    0    0
8  Up  Not Powered    0  Low  15400    0    0    0
9  Up  Not Powered    0  Low  15400    0    0    0
10 Up  Not Powered    0  Low  15400    0    0    0
11 Up  Not Powered    0  Low  15400    0    0    0
12 Up  Not Powered    0  Low  15400    0    0    0

-----<COMMAND>-----
[N]ext Page           Set PoE Port Admin [S]tatus
[P]revious Page      Set PoE Port Pr[i]ority
Set PoE Port Power [L]imit      [Q]uit to previous menu
Command> 
Enter the character in square brackets to select option

```

6.3.10.2 PoE Global Configuration

Globally configures switch to use PoE to provide power to connected IEEE 802.3af-compliant powered devices from all 10/100 Ethernet ports if the switch detects that there is no power on the circuit.

Map: Main Menu->Advanced Switch Configuration->Power Over Ethernet->Global Configuration

| | |
|--------------------|---|
| Power Usage: | Sets the power usage threshold for sending a trap. |
| Management Method: | Sets the action to take when the power sink over the power budget. One of the following two selections, 1) Low priority port will be shut down; 2) Deny next port connection. |
| Detection Method: | Enable or disable the power capacitor detection |

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Power Over Ethernet Configuration -> PoE Global Configuration Menu

Power Budget :                170W
Power Consumption :           6W
Power Usage Threshold For Sending Trap: 50 %
Power Management Method : Deny next port connection, regardless of priority
Power Detection Method : Capacitor detection enabled

----- <COMMAND> -----

Set Power [U]sage
Set Power [M]anagement Method
Set Power [D]etection Method
[Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

6.4 Statistics

Use this submenu to view statistics about the switch.

Map: Main Menu->Statistics

You can view the entire switch, select individual ports, refresh the screen to view current statistics or view statistics since the last reset.

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Main Menu -> Statistics Menu
Port: 1 Refresh: 300 Sec. Elapsed Time Since System Up: 000:02:59:47
<Counter Name>      <Total>      <Avg./s>
Total RX Bytes      0              0
Total RX Pkts       0              0
Good Broadcast      0              0
Good Multicast      0              0
CRC/Align Errors    0              0
Undersize Pkts      0              0
Oversize Pkts       0              0
Fragments           0              0
Jabbers             0              0
Collisions           0              0
64-Byte Pkts        0              0
65-127 Pkts         0              0
128-255 Pkts        0              0
256-511 Pkts        0              0
512-1023 Pkts       0              0
1024-1518 Pkts      0              0

----- <COMMAND> -----
[N]ext [P]revious [S]elect Port Re[f]resh Mode Since [R]eset [Q]uit
Command> 
Enter the character in square brackets to select option

```

6.5 Tools

This screen enables you to manage and monitor the PoE Switch.

Map: Main Menu->Tools

This page has seven submenus:

- TFTP Software Upgrade
- Configuration File Upload or Download
- System Reboot
- System Log
- Ping

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Main Menu -> Switch Tools Configuration

[T]FTP Software Upgrade
[C]onfiguration File Upload/Download
System [R]eboot
[P]ing Execution
System [L]og
[Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

6.5.1 TFTP Software Upgrade

This menu enables you to upgrade your switch to the new software release. Once the IP address of the TFTP and the name of the new software image file are properly configured, you can upgrade the software with command on this menu.

Map: Main Menu->Tools->TFTP Software Upgrade

Warning: The previous version of runtime image will be lost when the procedure completes.

The following procedure gives the steps to follow when using the web interface. The process is similar with either the CMI or CLI interfaces.

1. Go to Main Menu> Switch Tools Configuration> Software Upgrade Menu>TFTP Software Upgrade.
2. Set up the IP address and Image File Name.
3. Verify information such as the IP address for the TFTP Server and the file name of the new software image.
4. Verify the TFTP server and IP connection between server and switch are working properly.
5. Select Upgrade Image.

The switch downloads the image from TFTP Server and replaces the runtime image on Flash.

Note: Use a RS-232 serial port connection to the switch during the software upgrading procedure. When using a Telnet Session or web interface alone, your connection to the switch will not be available until the switch has completed its boot up and entered the Spanning Tree forwarding mode. This can take up to three minutes.

```

Terminal - telnet - 80x24
IC3624PWR Remote Management System
Switch Tools Configuration -> TFTP Software Upgrade

Image Version/Date:  1.0.0.01 / Oct 04 2004 15:38:33
TFTP Server IP:     0.0.0.0
Image File Name:

----- <COMMAND> -----

Set TFTP [S]erver IP Address
Set Image [F]ile Name
[U]pgrade Image
[Q]uit to previous menu

Command> 
Enter the character in square brackets to select option

```

6.5.2 Configuration File Upload/Download

Use this submenu to set addresses, establish configuration file names, upload and download files from one server to another.

Map: Main Menu->Tools->Configuration File Upload/Download

There are four submenus from this screen.

| | |
|-----------------------------|--|
| Set TFTP Server IP Address | Enter the server IP address to get the TFTP server |
| Set Configuration File Name | Enter the file name that you want to configuration |
| Upload Configuration File | Upload your configuration file |
| Download Configuration File | Download configuration file from TFTP server |

6.5.3 System Reboot

Use this submenu to establish the different types of system rebooting process.

Map: Main Menu->Tools->System Reboot

When the system reboots, the following options are available.

Reboot Type:

| | |
|---|--|
| N | Normal: Reboots with current runtime code and configuration. |
| F | Factory-Default: Runs as the default configuration after reboot. Use if previous configuration failed. |
| I | Factory Default Except IP: Runs as the default configuration after reboot except IP configuration |

6.5.4 Ping Execution

Use this submenu to ping the system to determine if the switch is responding.

Map: Main Menu->Tools->Ping

There are five options available from this submenu.

- Target IP Address
- Member of Requests
- Timeout Value
- Execute Ping
- Stop Ping

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Switch Tools Configuration -> Ping Execution

Target IP Address:    0.0.0.0
Number of Requests:  10
Timeout Value:       3 Sec.
===== Result =====

-----<COMMAND>-----
Set Target [I]P Address           [E]xecute Ping
Set [N]umber of Requests         [S]top Ping
Set [T]imeout Value              [Q]uit to previous menu
Command> [ ]
Enter the character in square brackets to select option

```

6.5.5 System Log

Use this submenu to observe system behavior. You can clear the system log by selecting Clear System Log.

Map: Main Menu->Tools->System

```

Terminal — telnet — 80x24
IC3624PWR Remote Management System
Switch Tools Configuration -> System Log Menu

Entry  Time(YYYY/MM/DD HH:MM:SS)  Event
-----
  1  0000/00/00 00:00:14  Configuration changed
  2  0000/00/00 00:00:17  Reboot: Factory Default
  3  0000/00/00 00:00:20  (Bridge) Topology Change
  4  0000/00/00 00:00:38  Login from console
  5  0000/00/00 00:12:12  Login from console
  6  0000/00/00 00:35:04  (Bridge) Topology Change
  7  0000/00/00 00:35:06  (Bridge) Topology Change
  8  0000/00/00 00:31:59  (Bridge) Topology Change
  9  0000/00/00 00:33:21  Login from console
 10  0000/00/00 00:33:54  Login from console

-----<COMMAND>-----
[N]ext Page
[P]revious Page
[C]lear System Log
[Q]uit to previous menu

Command> [ ]
Enter the character in square brackets to select option

```

6.6 Save Configuration

Use this submenu to save the changed settings to the Flash memory after making any changes to the screens within the console interface.

Map: Main Menu->Tools->Save Configuration to Flash

To save the configuration to Flash memory select Save Configuration and then press either 'Enter' or 'Y'.

6.7 Run CLI

Use this submenu to configure the switch using the command line interface (CLI). To return to the menu-driven interface type "exit".

Appendix A: Basic Troubleshooting

In the event the switch does not operate properly, follow the troubleshooting tips below. If you need more help contact Asante technical support at www.asante.com/support.

A.1 Diagnosing Switch Indicators

Refer to the following troubleshooting chart for information about the diagnostic LEDs.

| Problem | Possible Solutions |
|---------------------------|---|
| The Power LED is not lit. | <p>LED will turn off during system initialization.</p> <p>Check the power connection. Plug the power cord into another known working AC outlet.</p> <p>The primary power supply has failed. Install the optional emergency power supply and have the primary power supply serviced as soon as possible.</p> |
| Link LED is not lit | <p>Verify that the switch and attached device are powered on.</p> <p>Check the connection between the switch and corresponding device.</p> <p>Verify that the proper cable type is used and the length does not exceed specified limits.</p> <p>Check the adapter on the attached device and cable connections for possible defects. Replace the defective adapter or cable if necessary.</p> |

A.2 Power and Cooling Problems

If the power indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or internal power supply. However, if the unit powers off after running for a while, check for loose power connections, power losses or surges at the power outlet, and verify that the fans on the unit are unobstructed and running prior to shutdown. If you still cannot isolate the problem, then the internal power supply may be defective.

A.3 Installation

Verify that all system components are properly installed. If one or more components appear to be malfunctioning (for example the power cord or network cabling), test them in an alternate environment where you are sure that all the other components are functioning properly.

A.4 In-Band Access

You can access the management agent in the switch from anywhere within the attached network using Telnet, a Web browser, or other network management software tools. Do this by configuring the switch with a valid IP address, subnet mask, and default gateway. If you can not establish a link to the management agent, verify that there is a valid network connection, you entered the correct IP address, and that the port through which you are connecting to the switch has not been disabled. If it has not been disabled, check the network cabling that runs between the remote location and the switch.

Caution: The management agent can accept up to four simultaneous Telnet sessions. If you are at maximum number of sessions, an additional Telnet connection can not log into the system.

Appendix B: Specifications

The sections below list the features and product specifications for the IntraCore IC3624PWR PoE switch.

| Physical Characteristics | |
|---------------------------------|--|
| Ports | 24 10/100BaseTX with auto-negotiation 2 Combination Ports (RJ-45/SFP), 10/100/1000BaseT or 1000BaseX |
| Network Interface | RJ-45 connector, auto MDI/X 10BaseT: RJ-45 (100-ohm, UTP cable; Categories 3, 4, 5) Maximum Cable Length - 100 m (328 ft) 100BaseTX: RJ-45 (100-ohm, UTP cable; Category 5) Maximum Cable Length - 100 m (328 ft) 1000BaseT: RJ-45 (100-ohm, UTP or STP cable; Category 5, 5e, or 6) Maximum Cable Length - 100 m (328 ft) |
| LEDs | System: Power (Power Supply) Port: Link/Act (Link/Activity) |
| Weight | 9.5 lb (4.3 Kg) |
| Size | 17.3 x 9.9 x 1.7 inches (440 x 253 x 43.2mm) |
| Temperature | Operating: 32o to 104o F (0o to 40o C) |
| Humidity | Operating: 10% to 90% non-condensing |
| AC Input | 100-240 VAC, 50/60 Hz, maximum 225 watts |
| Performance | |
| Switch Architecture | Non-blocking 8.8 Gbps |
| Forwarding MAC Table | Up to 8K unicast addresses with automatic learning and aging |
| Throughput | Wire-speed Gigabit switching (1,488,000 pps) and Fast Ethernet switching (148,800) |
| Flow Control | IEEE 802.3x flow control (full duplex) and back pressure (half-duplex) |
| Switch Architecture | Non-blocking 8.8 Gbps switch fabric |
| Forwarding MAC Table Packet | Up to 8K unicast addresses with automatic learning and aging |
| Buffer | 256 KB |

| L2+ Switching | |
|----------------------------|--|
| Virtual LANs | IEEE 802.1q, 256 VLANs |
| Spanning Tree | IEEE 802.1d (STP), IEEE 802.1s (multiple), IEEE 802.1w (rapid reconfiguration), fast link |
| Flow Control | IEEE 802.3x |
| Link Aggregation | IEEE 802.3ad, LACP, up to 6 trunks |
| Authentication | IEEE 802.1x per port access control |
| Quality of Service | IEEE 802.1p DiffServ and IP ToS |
| Power over Ethernet | Up to 15.4 watts per 10/100 port; 180 watts total |
| Management Features | |
| In-Band | Telnet, HTTP or SNMP manager. Software loading TFTP |
| Out-of-Band | RS-232 DB-9 console port. Software loading XModem |
| Standards | |
| IEEE, ISO, IEC | IEEE 802.3 10BaseT IEEE 802.3u 100BaseTX IEEE 802.3ab 1000BaseT IEEE 802.3z 1000BaseSX/LX IEEE 802.3x full duplex flow control |
| Compliances | |
| CE Mark | Standard |
| Emissions | FCC Class A |
| Safety | UL |

Appendix C: Cables and Pin Assignments

This Appendix describes the information on 10BaseT/100BaseTX, 1000BaseT, and testing for existing Category 5 cables.

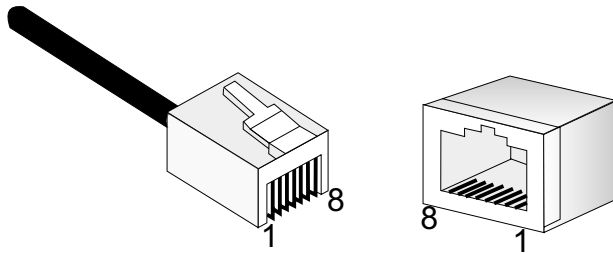
C.1 Twisted-Pair Cable and Pin Assignments

For 10BaseT/100BaseTX connections, a twisted-pair cable must have two pairs of wires. Each wire pair is identified by two different colors. For example, one green wire and another green with white stripes. You must attach an RJ-45 connector to both ends of the cable.

Warning: DO NOT plug a phone jack connector into any RJ-45 port. This will damage the switch. Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

Caution: Attach each wire pair to the RJ-45 connectors in a specific orientation. (See “ 4.1.1 Cable Guidelines” for more information.)

The figure below illustrates how the pins on the RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.



C.1.1 Pin Assignments for 10BaseT/100BaseTX

Use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ-45 connections: 100-ohm Category 3, 4 or 5 cable for 10 Mbps connections or 100-ohm Category 5 cable for 100 Mbps connections. Additionally, the length of any twisted-pair connection does not exceed 100 meters (328 feet).

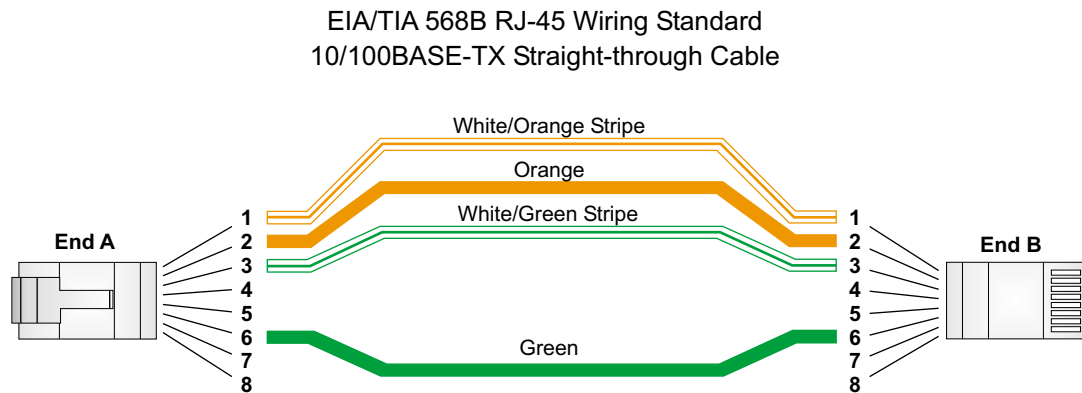
The RJ-45 ports on the switch base unit support automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs. In straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3, and 6 at the other end of the cable. When using any RJ-45 port on this switch, you can use either straight-through or crossover cable.

| Pin | Signal Name | X Signal Name |
|------------|---------------------------|---------------------------|
| 1 | Transmit Data plus (TD+) | Receive Data plus (RD+) |
| 2 | Transmit Data minus (TD-) | Receive Data minus (RD-) |
| 3 | Receive Data plus (RD+) | Transmit Data plus (TD+) |
| 6 | Receive Data minus (RD-) | Transmit Data minus (TD-) |
| 4, 5, 7, 8 | N/A | N/A |

Note: The “+” and “-” signs represent the polarity of the wires that make up each wire pair.

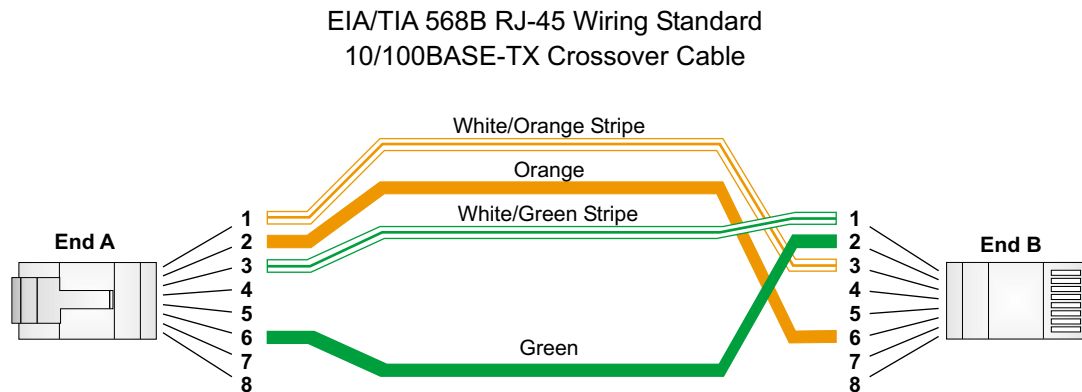
C.1.2 Straight-Through Wiring

If the twisted-pair cable is to join two ports and only one of the ports has an internal crossover (MDI-X), the two pairs of wires must be straight-through. (When auto-negotiation is enabled for any RJ-45 port on this switch, you can use either straight-through or crossover cable to connect to any device type.)



C.1.3 Crossover Wiring

If the twisted-pair cable is to join two ports and both ports have the same indicator (MDI or MDI-X) a crossover must be implemented in the wiring. (When auto-negotiation is enabled for any RJ-45 port on this switch, you can use either the straight-through or the crossover cable to connect to any device type.)



C.2 Pin Assignments for 1000BaseT Pin

All 1000BaseT ports support automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs.

The table below shows the 1000BaseT MDI and MDI-X port pinouts. These ports require that all four pairs of wires be connected. Note that for 1000BaseT operation, all four pairs of wires are used for both transmit and receive.

Use 100-ohm Category 5, 5e or 6 unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for 1000BaseT connections. The length of any twisted-pair connection must not exceed 100 meters (328 feet).

| Pin | MDI Signal Name | MDI-X Signal Name |
|-----|--|--|
| 1 | Bi-directional Data One Plus (BI_D1+) | Bi-directional Data Two Plus (BI_D2+) |
| 2 | Bi-directional Data One Minus (BI_D1-) | Bi-directional Data Two Minus (BI_D2-) |
| 3 | Bi-directional Data Two Plus (BI_D2+) | Bi-directional Data One Plus (BI_D1+) |
| 4 | Bi-directional Data Three Plus (BI_D3+) | Bi-directional Data Four Plus (BI_D4+) |
| 5 | Bi-directional Data Three Minus (BI_D3-) | Bi-directional Data Four Minus (BI_D4-) |
| 6 | Bi-directional Data Two Minus (BI_D2-) | Bi-directional Data One Minus (BI_D1-) |
| 7 | Bi-directional Data Four Plus (BI_D4+) | Bi-directional Data Three Plus (BI_D3+) |
| 8 | Bi-directional Data Four Minus (BI_D4-) | Bi-directional Data Three Minus (BI_D3-) |

C.3 Cable Testing for Existing Category 5 Cable

Installed Category 5 cabling must pass tests for Attenuation, Near-End Crosstalk (NEXT), and Far-End Crosstalk (FEXT). This cable testing specifications are contained in the ANSI/TIA/EIA-TSB-67 standard. Cables must pass test parameters for Return Loss and Equal-Level Far-End Crosstalk (ELFEXT). These tests are contained in the ANSI/TIA/EIA-TSB-95 Bulletin, "The Additional Transmission Performance Guidelines for 100 Ohm 4-Pair Category 5 Cabling."

Note: When testing the cable installation, be sure to include all patch cables between switches and end devices.

C.3.1 Adjusting Existing Category 5 Cabling to Run 1000BaseT

If your existing Category 5 installation does not meet one of the test parameters for 1000BaseT, follow these measures to correct the problem:

Replace any Category 5 patch cables with high-performance Category 5e or Category 6 cables.

Reduce the number of connectors used in the link.

Reconnect some of the connectors in the link.

C.4 Fiber Standards

The current TIA (Telecommunications Industry Association) 568-A specification on optical fiber cabling consists of one recognized cable type for horizontal subsystems and two cable types for backbone subsystems.

Horizontal 62.5/125 micron multimode (two fibers per outlet).

Backbone 62.5/125 micron multimode or singlemode.

TIA 568-B allows the use of 50/125 micron multimode optical fiber in both the horizontal and backbone in addition to the types listed above. All optical fiber components and installation practices must meet applicable building and safety codes.

Appendix D: FCC Compliance and Warranty Statements

D.1 FCC Compliance Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

D.2 Important Safety Instructions

Caution: Do not use an RJ-11 (telephone) cable to connect network equipment.

Read all of these instructions.

Save these instructions for later use.

Follow all warnings and instructions marked on the product.

Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.

Do not use this product near water.

Do not place this product on an unstable cart or stand. The product may fall, causing serious damage to the product.

The air vent should never be blocked (such as by placing the product on a bed, sofa or rug). This product should never be placed near or over a radiator or heat register. This product should not be placed in a built-in installation unless proper ventilation is provided.

This product should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.

This product is equipped with a three-wire grounding type plug, which is a plug having a third (grounding) pin. This plug will only fit into a grounding type power outlet. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your outlet. Do not defeat the purpose of the grounding type plug.

Do not allow anything to rest on the power cord. Do not place this product where people will walk on the cord.

If an extension cord is used with this product, make sure that the total ampere ratings on the products into the extension cord do not exceed the extension cord ampere rating. Also make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.

Never push objects of any kind into this product through air ventilation slots as they may touch dangerous voltage points or short out parts that could result in a risk of fire or electric shock. Never spill liquid of any kind on the product.

Do not attempt to service this product yourself, as opening or removing covers may expose you to dangerous voltage points or other risks. Refer all servicing to service personnel.

D.3 IntraCore Warranty Statement

Products: IntraCore IC3624PWR

Duration: 3 years

Advanced Warranty United States: Second Business Day

Replacement: Other Countries: See your local distributor or reseller.

Asante Technologies warrants (to the original end-user purchaser) the covered IntraCore products against defects in materials and workmanship for the period specified above. If Asante receives notice of such defects during the warranty period, Asante will, at its option, either repair or replace products that prove to be defective. Replacement products may be either new or like-new.

Asante warrants that Asante software will not fail to execute its programming instructions, for the period specified previously, due to defects in material and workmanship when properly installed and used. If Asante receives notice of such defects during the warranty period, Asante will replace software media that does not execute its programming instructions due to such defects.

Asante does not warrant that the operation of Asante products will be uninterrupted or error free. If Asante is unable, within a reasonable time, to repair or replace any product to a condition as warranted, customer would be entitled to a refund of the pro-rated purchase price upon prompt return of the product.

Asante products may contain remanufactured parts equivalent to new in performance.

The warranty period begins on the date of delivery or on the date of installation if installed by Asante.

Warranty does not apply to defects resulting from (a) improper or inadequate maintenance or calibration, (b) software, interfacing, parts, or supplies not received from Asante, (c) unauthorized modification or misuse, (d) operation outside of the published environmental specifications for the product, or (e) improper site preparation or maintenance. This warranty expressly excludes problems arising from compatibility with other vendors' products, or future compatibility due to third-party software or driver updates.

TO THE EXTENT ALLOWED BY LOCAL LAW, THE PREVIOUS WARRANTIES ARE EXCLUSIVE AND NO OTHER WARRANTY OR CONDITION, WHETHER WRITTEN OR ORAL, IS EXPRESSED OR IMPLIED AND ASANTÉ SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, AND FITNESS FOR A PARTICULAR PURPOSE.

Asante will be liable for damage to tangible property per incident up to the greater of \$10,000 or the actual amount paid for the product that is the subject of the claim, and for damages for bodily injury or death, to the extent that all such damages are determined by a court of competent jurisdiction to have been directly caused by a defective Asante product.

TO THE EXTENT ALLOWED BY LOCAL LAW, THE REMEDIES IN THIS WARRANTY STATEMENT ARE THE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES. EXCEPT AS INDICATED PREVIOUSLY, IN NO EVENT WILL ASANTÉ OR ITS SUPPLIERS BE LIABLE FOR LOSS OF DATA OR FOR DIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL (INCLUDING LOST PROFIT OR DATA), OR OTHER DAMAGE, WHETHER BASED IN CONTRACT, OR OTHERWISE.

Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages or imitations on how long an implied warranty lasts, so the previous limitations or exclusions may not apply to you. This warranty gives you specific legal rights, and you may have other rights, which vary from jurisdiction to jurisdiction.

Appendix E. Online Warranty Registration

Please register the switch online at www.asante.com/support/warranty/index.html. By doing so, you'll be entitled to special offers, up-to-date information, and important product bulletins.



NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES



BUSINESS REPLY MAIL
FIRST CLASS MAIL PERMIT NO. 4196 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

REGISTRATION CARDS
ASANTE TECHNOLOGIES INC
2223 Old Oakland Road
SAN JOSE CA 95131-1402



Fold at line and tape closed. Do not staple. No postage required.

Asante Product Registration Card

| |
|-----------------------|
| Name |
| Title |
| Company |
| Address 1 |
| Address 2 |
| City |
| State |
| Zip/Postal |
| Country |
| Phone |
| Fax |
| Email |
| Date of Purchase |
| Asante Part Number |
| Product Serial Number |

To register your Asante product online, please visit:
<http://www.asante.com/support/registration.html>